
Amazon Relational Database Service

User Guide



Amazon Relational Database Service: User Guide

Copyright © 2022 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon RDS?	1
Overview	1
Amazon EC2 and on-premises databases	1
Amazon RDS and Amazon EC2	2
Amazon RDS Custom for Oracle and Microsoft SQL Server	3
Amazon RDS on AWS Outposts	3
DB instances	3
DB engines	4
DB instance classes	4
DB instance storage	4
Amazon Virtual Private Cloud (Amazon VPC)	5
AWS Regions and Availability Zones	5
Security	5
Monitoring an Amazon RDS DB instance	5
How to work with Amazon RDS	5
AWS Management Console	6
Command line interface	6
Programming with Amazon RDS	6
How you are charged for Amazon RDS	6
What's next?	6
Getting started	6
Topics specific to database engines	6
DB instances	8
DB instance classes	10
DB instance class types	10
Supported DB engines	12
Determining DB instance class support in AWS Regions	39
Changing your DB instance class	42
Configuring the processor	42
Hardware specifications	55
DB instance storage	64
Storage types	64
General Purpose SSD storage	64
Provisioned IOPS storage	66
Comparing SSD storage types	68
Magnetic storage	68
Monitoring storage performance	69
Factors that affect storage performance	69
Regions, Availability Zones, and Local Zones	72
AWS Regions	73
Availability Zones	75
Local Zones	76
Supported Amazon RDS features by Region and engine	77
Table conventions	77
Feature quick reference	77
Cross-Region automated backups	78
Cross-Region read replicas	83
Database activity streams	85
Dual-stack mode	88
Export snapshots to S3	95
IAM database authentication	99
Kerberos authentication	101
Multi-AZ DB clusters	107
Performance Insights	110

RDS Custom	110
Amazon RDS Proxy	114
Engine-native features	120
Multi-AZ deployments	121
Multi-AZ DB instance deployments	122
Multi-AZ DB cluster deployments	127
DB instance billing for Amazon RDS	138
On-Demand DB instances	139
Reserved DB instances	140
Setting up	148
Sign up for an AWS account	148
Create an administrative user	148
Create IAM user access keys	149
Determine requirements	150
Provide access to your DB instance	151
Getting started	153
Creating a MariaDB DB instance and connecting to a database	154
Creating a MariaDB DB instance	154
Connecting to a database on a DB instance running MariaDB	158
Deleting a DB instance	161
Creating a SQL Server DB instance and connecting to it	162
Creating a sample SQL Server DB instance	162
Connecting to your sample DB instance	166
Exploring your sample DB instance	169
Deleting your sample DB instance	170
Creating a MySQL DB instance and connecting to a database	172
Creating a MySQL DB instance	172
Connecting to a database on a DB instance running MySQL	176
Deleting a DB instance	179
Creating an Oracle DB instance and connecting to a database	180
Creating a sample Oracle DB instance	180
Connecting to your sample DB instance	184
Deleting your sample DB instance	186
Creating a PostgreSQL DB instance and connecting to a database	187
Creating a PostgreSQL DB instance	187
Connecting to a PostgreSQL DB instance	191
Deleting a DB instance	197
Tutorial: Create a web server and an Amazon RDS DB instance	198
Launch an EC2 instance	199
Create a DB instance	203
Install a web server	207
Tutorials and sample code	214
Tutorials in this guide	214
Tutorials in other AWS guides	215
Tutorials and sample code in GitHub	215
Best practices for Amazon RDS	216
Amazon RDS basic operational guidelines	216
DB instance RAM recommendations	217
Using Enhanced Monitoring to identify operating system issues	217
Using metrics to identify performance issues	217
Viewing performance metrics	217
Evaluating performance metrics	220
Tuning queries	221
Best practices for working with MySQL	222
Table size	222
Number of tables	222
Storage engine	223

Best practices for working with MariaDB	223
Table size	223
Number of tables	224
Storage engine	224
Best practices for working with Oracle	224
Best practices for working with PostgreSQL	224
Loading data into a PostgreSQL DB instance	225
Working with the PostgreSQL autovacuum feature	225
Amazon RDS for PostgreSQL best practices video	226
Best practices for working with SQL Server	226
Amazon RDS for SQL Server best practices video	227
Working with DB parameter groups	227
Best practices for automating DB instance creation	227
Amazon RDS new features and best practices presentation video	228
Configuring a DB instance	229
Creating a DB instance	230
Prerequisites	230
Creating a DB instance	233
Available settings	237
Creating a Multi-AZ DB cluster	252
Prerequisites	252
Creating a DB cluster	255
Available settings	258
Nonapplicable settings	265
Creating resources with AWS CloudFormation	266
RDS and AWS CloudFormation templates	266
Learn more about AWS CloudFormation	266
Connecting to a DB instance	267
Finding the connection information	267
Database authentication options	270
Encrypted connections	271
Scenarios for accessing a DB instance	271
Connecting to a DB instance running a specific DB engine	271
Managing connections with RDS Proxy	272
Working with option groups	273
Option groups overview	273
Creating an option group	274
Copying an option group	276
Adding an option to an option group	277
Listing the options and option settings for an option group	281
Modifying an option setting	282
Removing an option from an option group	285
Deleting an option group	286
Working with parameter groups	289
Working with DB parameter groups	291
Working with DB cluster parameter groups	302
Comparing parameter groups	310
Specifying DB parameters	310
Managing a DB instance	316
Stopping a DB instance	317
Benefits	318
Limitations	318
Option and parameter group considerations	318
Public IP address	318
Stopping a DB instance	318
Starting a DB instance	320
Connecting an EC2 instance	321

Overview	321
Connecting an EC2 instance	324
Viewing connecting compute resources	326
Modifying a DB instance	327
Apply Immediately setting	328
Available settings	328
Modifying a Multi-AZ DB cluster	341
Apply Immediately setting	342
Available settings	342
Nonapplicable settings	348
Maintaining a DB instance	350
Viewing pending maintenance	350
Applying updates	352
Maintenance for Multi-AZ deployments	353
The maintenance window	354
Adjusting the maintenance window for a DB instance	355
Working with operating system updates	356
Upgrading the engine version	360
Manually upgrading the engine version	360
Automatically upgrading the minor engine version	362
Renaming a DB instance	364
Renaming to replace an existing DB instance	364
Rebooting a DB instance	366
Rebooting Multi-AZ DB clusters	368
Working with read replicas	370
Overview	372
Creating a read replica	375
Promoting a read replica	377
Monitoring read replication	380
Cross-Region read replicas	383
Tagging RDS resources	392
Overview	392
Using tags for access control with IAM	393
Using tags to produce detailed billing reports	393
Adding, listing, and removing tags	394
Using the AWS Tag Editor	396
Copying tags to DB instance snapshots	396
Tutorial: Use tags to specify which DB instances to stop	397
Enabling backups	399
Working with ARNs	402
Constructing an ARN	402
Getting an existing ARN	406
Working with storage	410
Increasing DB instance storage capacity	410
Managing capacity automatically with storage autoscaling	412
Modifying Provisioned IOPS settings	416
I/O-intensive storage modifications	418
Modifying General Purpose (gp3) settings	418
Deleting a DB instance	421
Deletion protection	421
Final snapshots and retained backups	421
Deleting a DB instance	422
Deleting a Multi-AZ DB cluster	424
Backing up and restoring a DB instance	426
Working with backups	427
Backup storage	427
Backup window	428

Backup retention period	429
Enabling automated backups	429
Retaining automated backups	431
Deleting retained automated backups	433
Disabling automated backups	434
Using AWS Backup	435
Unsupported MySQL storage engines	435
Unsupported MariaDB storage engines	436
Cross-Region automated backups	437
Region and version availability	437
Source and destination AWS Region support	437
Enabling cross-Region automated backups	439
Finding information about replicated backups	441
Point-in-time recovery from a replicated backup	444
Stopping backup replication	445
Deleting replicated backups	446
Creating a DB snapshot	448
Creating a Multi-AZ DB cluster snapshot	450
Restoring from a DB snapshot	452
Parameter groups	452
Security groups	452
Option groups	453
Tagging	453
Microsoft SQL Server	453
Oracle Database	454
Restoring from a snapshot	454
Restoring from a snapshot to a Multi-AZ DB cluster	456
Copying a DB snapshot	458
Limitations	458
Snapshot retention	458
Copying shared snapshots	458
Handling encryption	459
Incremental snapshot copying	459
Cross-Region copying	460
Option groups	463
Parameter groups	463
Copying a DB snapshot	464
Sharing a DB snapshot	472
Sharing public snapshots	473
Sharing encrypted snapshots	474
Sharing a snapshot	476
Exporting DB snapshot data to Amazon S3	481
Region and version availability	481
Limitations	481
Overview of exporting snapshot data	482
Setting up access to an S3 bucket	483
Using a cross-account KMS key	485
Exporting a DB snapshot	486
Monitoring snapshot exports	489
Canceling a snapshot export	490
Failure messages	491
Troubleshooting PostgreSQL permissions errors	492
File naming convention	492
Data conversion	493
Point-in-time recovery	499
Restoring a Multi-AZ DB cluster to a specified time	502
Deleting a DB snapshot	505

Deleting a DB snapshot	505
Tutorial: Restore a DB instance from a DB snapshot	507
Restoring a DB instance from a DB snapshot	507
Monitoring metrics in a DB instance	510
Overview of monitoring	511
Monitoring plan	511
Performance baseline	511
Performance guidelines	511
Monitoring tools	512
Viewing instance status and recommendations	515
Viewing Amazon RDS DB instance status	516
Viewing Amazon RDS recommendations	520
Viewing metrics in the Amazon RDS console	525
Monitoring RDS with CloudWatch	528
Overview of Amazon RDS and Amazon CloudWatch	529
Viewing CloudWatch metrics	530
Creating CloudWatch alarms	535
Tutorial: Creating a CloudWatch alarm for DB cluster replica lag	536
Monitoring DB load with Performance Insights	543
Overview of Performance Insights	543
Turning Performance Insights on and off	549
Turning on the Performance Schema for MariaDB or MySQL	553
Performance Insights policies	556
Analyzing metrics with the Performance Insights dashboard	559
Retrieving metrics with the Performance Insights API	584
Logging Performance Insights calls using AWS CloudTrail	598
Monitoring the OS with Enhanced Monitoring	600
Overview of Enhanced Monitoring	600
Setting up and enabling Enhanced Monitoring	601
Viewing OS metrics in the RDS console	605
Viewing OS metrics using CloudWatch Logs	608
RDS metrics reference	609
CloudWatch metrics for RDS	609
CloudWatch dimensions for RDS	616
CloudWatch metrics for Performance Insights	617
Counter metrics for Performance Insights	618
SQL statistics for Performance Insights	628
OS metrics in Enhanced Monitoring	633
Monitoring events, logs, and database activity streams	642
Viewing logs, events, and streams in the Amazon RDS console	642
Monitoring RDS events	646
Overview of events for Amazon RDS	646
Viewing Amazon RDS events	647
Working with Amazon RDS event notification	650
Creating a rule that triggers on an Amazon RDS event	664
Amazon RDS event categories and event messages	668
Monitoring RDS logs	680
Viewing and listing database log files	680
Downloading a database log file	681
Watching a database log file	682
Publishing to CloudWatch Logs	683
Reading log file contents using REST	685
MariaDB database log files	687
Microsoft SQL Server database log files	696
MySQL database log files	700
Oracle database log files	709
PostgreSQL database log files	716

Monitoring RDS API calls in CloudTrail	725
CloudTrail integration with Amazon RDS	725
Amazon RDS log file entries	725
Monitoring Oracle with Database Activity Streams	729
Overview	729
Configuring Oracle unified auditing	732
Starting a database activity stream	732
Modifying a database activity stream	734
Getting the activity stream status	736
Stopping a database activity stream	737
Monitoring activity streams	738
Managing access to activity streams	752
Working with Amazon RDS Custom	755
Database customization challenge	755
RDS Custom management model and benefits	756
Shared responsibility model	756
Key benefits of RDS Custom	758
RDS Custom architecture	758
VPC	759
Amazon S3	759
AWS CloudTrail	760
RDS Custom automation and monitoring	760
Security considerations for RDS Custom	762
Working with RDS Custom for Oracle	763
RDS Custom for Oracle workflow	763
RDS Custom for Oracle requirements and limitations	766
Setting up your RDS Custom for Oracle environment	768
Working with CEVs for RDS Custom for Oracle	781
Configuring an RDS Custom for Oracle DB instance	807
Managing an RDS Custom for Oracle DB instance	816
Working with RDS Custom for Oracle replicas	826
Backing up and restoring an RDS Custom for Oracle DB instance	831
Upgrading a DB instance for RDS Custom for Oracle	838
Working with RDS Custom for SQL Server	843
RDS Custom for SQL Server workflow	843
RDS Custom for SQL Server requirements and limitations	845
Setting up your RDS Custom for SQL Server environment	847
Creating and connecting to an RDS Custom for SQL Server DB instance	860
Managing an RDS Custom for SQL Server DB instance	868
Backing up and restoring an RDS Custom for SQL Server DB instance	877
Migrating an on-premises database to RDS Custom for SQL Server	885
Upgrading a DB instance for RDS Custom for SQL Server	888
Troubleshooting RDS Custom	889
Viewing RDS Custom events	889
Subscribing to event notifications	889
Troubleshooting CEV creation	890
Support perimeter and unsupported configurations	891
Fixing unsupported configurations	891
How Amazon RDS Custom replaces an impaired host	897
Troubleshooting RDS Custom for Oracle upgrade issues	899
Troubleshooting RDS Custom for Oracle replica promotion	900
Troubleshooting RDS Custom for Oracle replica creation	900
Working with RDS on AWS Outposts	902
Prerequisites	902
Support for Amazon RDS features	904
Supported DB instance classes	907
Customer-owned IP addresses	909

Using ColPs	909
Limitations	910
Multi-AZ deployments	911
Working with the shared responsibility model	911
Improving availability	911
Prerequisites	912
Working with API operations for Amazon EC2 permissions	913
Creating DB instances for RDS on Outposts	914
Considerations for restoring DB instances	920
Using RDS Proxy	921
Region and version availability	921
Quotas and limitations	921
RDS for MariaDB limitations	922
RDS for SQL Server limitations	923
MySQL limitations	923
PostgreSQL limitations	924
Planning where to use RDS Proxy	924
RDS Proxy concepts and terminology	925
Overview of RDS Proxy concepts	925
Connection pooling	926
Security	926
Failover	928
Transactions	928
Getting started with RDS Proxy	929
Setting up network prerequisites	929
Setting up database credentials in Secrets Manager	931
Setting up IAM policies	932
Creating an RDS Proxy	934
Viewing an RDS Proxy	938
Connecting through RDS Proxy	939
Managing an RDS Proxy	941
Modifying an RDS Proxy	942
Adding a database user	946
Changing database passwords	946
Configuring connection settings	946
Avoiding pinning	948
Deleting an RDS Proxy	952
Working with RDS Proxy endpoints	952
Overview of proxy endpoints	953
Reader endpoints	953
Accessing Aurora and RDS databases across VPCs	954
Creating a proxy endpoint	954
Viewing proxy endpoints	956
Modifying a proxy endpoint	957
Deleting a proxy endpoint	958
Limitations for proxy endpoints	959
Monitoring RDS Proxy with CloudWatch	959
Working with RDS Proxy events	964
RDS Proxy events	964
RDS Proxy examples	965
Troubleshooting RDS Proxy	967
Verifying connectivity for a proxy	967
Common issues and solutions	968
Using RDS Proxy with AWS CloudFormation	972
MariaDB on Amazon RDS	974
MariaDB feature support	975
MariaDB major versions	975

Supported storage engines	979
Cache warming	980
Features not supported	981
MariaDB versions	982
Supported MariaDB versions	982
MariaDB release calendar	983
MariaDB 10.3 end of life	984
MariaDB 10.2 end of life	984
Deprecated MariaDB versions	985
Connecting to a DB instance running MariaDB	986
Finding the connection information	986
Connecting from the MySQL command-line client (unencrypted)	989
Troubleshooting	990
Securing MariaDB connections	991
MariaDB security	991
Encrypting with SSL/TLS	992
Using new SSL/TLS certificates	994
Upgrading the MariaDB DB engine	998
Overview	998
Major version upgrades	999
Upgrading a MariaDB DB instance	1000
Automatic minor version upgrades	1000
Importing data into a MariaDB DB instance	1003
Importing data from an external database	1004
Importing data to a DB instance with reduced downtime	1006
Importing data from any source	1019
Working with MariaDB replication	1024
Working with MariaDB read replicas	1024
Configuring GTID-based replication with an external source instance	1034
Configuring binary log file position replication with an external source instance	1036
Options for MariaDB	1040
MariaDB Audit Plugin support	1040
Parameters for MariaDB	1043
Viewing MariaDB parameters	1043
MySQL parameters that aren't available	1044
Migrating data from a MySQL DB snapshot to a MariaDB DB instance	1046
Performing the migration	1046
Incompatibilities between MariaDB and MySQL	1048
MariaDB on Amazon RDS SQL reference	1049
mysql.rds_replica_status	1049
mysql.rds_set_external_master_gtid	1050
mysql.rds_kill_query_id	1052
Local time zone	1054
MariaDB limitations	1056
File size limits	1056
InnoDB reserved word	1057
Microsoft SQL Server on Amazon RDS	1058
Common management tasks	1059
Limitations	1060
DB instance class support	1062
Security	1064
Compliance programs	1065
HIPAA	1065
SSL support	1066
Version support	1066
Version management	1067
Database engine patches and versions	1067

Deprecation schedule	1067
Feature support	1068
SQL Server 2019 features	1068
SQL Server 2017 features	1069
SQL Server 2016 features	1069
SQL Server 2014 features	1069
SQL Server 2012 end of support on Amazon RDS	1070
SQL Server 2008 R2 end of support on Amazon RDS	1070
CDC support	1070
Features not supported and features with limited support	1071
Multi-AZ deployments	1071
Using TDE	1072
Functions and stored procedures	1072
Local time zone	1074
Supported time zones	1075
Licensing SQL Server on Amazon RDS	1083
Restoring license-terminated DB instances	1083
SQL Server Developer Edition	1083
Connecting to a DB instance running SQL Server	1084
Before you connect	1084
Finding the DB instance endpoint and port number	1084
Connecting to your DB instance with SSMS	1085
Connecting to your DB instance with SQL Workbench/J	1087
Security group considerations	1089
Troubleshooting	1089
Updating applications for new SSL/TLS certificates	1091
Determining whether any applications are connecting to your Microsoft SQL Server DB instance using SSL	1091
Determining whether a client requires certificate verification in order to connect	1092
Updating your application trust store	1093
Upgrading the SQL Server DB engine	1094
Overview	1095
Major version upgrades	1095
Multi-AZ and in-memory optimization considerations	1096
Option group considerations	1097
Parameter group considerations	1097
Testing an upgrade	1097
Upgrading a SQL server DB instance	1098
Upgrading deprecated DB instances before support ends	1098
Importing and exporting SQL Server databases	1099
Limitations and recommendations	1100
Setting up	1101
Using native backup and restore	1105
Compressing backup files	1115
Troubleshooting	1115
Importing and exporting SQL Server data using other methods	1117
Working with SQL Server read replicas	1126
Configuring read replicas for SQL Server	1126
Read replica limitations with SQL Server	1126
Option considerations	1127
Troubleshooting a SQL Server read replica problem	1128
Multi-AZ for RDS for SQL Server	1129
Adding Multi-AZ to a SQL Server DB instance	1130
Removing Multi-AZ from a SQL Server DB instance	1130
Limitations, notes, and recommendations	1130
Determining the location of the secondary	1132
Migrating to Always On AGs	1133

Additional features for SQL Server	1134
Using SSL with a SQL Server DB instance	1135
Configuring security protocols and ciphers	1138
Using Windows Authentication with a SQL Server DB instance	1143
Amazon S3 integration	1153
Using Database Mail	1167
Instance store support for tempdb	1178
Using extended events	1180
Access to transaction log backups	1183
Options for SQL Server	1203
Listing the available options for SQL Server versions and editions	1204
Linked Servers with Oracle OLEDB	1206
Native backup and restore	1214
Transparent Data Encryption	1217
SQL Server Audit	1225
SQL Server Analysis Services	1232
SQL Server Integration Services	1251
SQL Server Reporting Services	1266
Microsoft Distributed Transaction Coordinator	1279
Common DBA tasks for SQL Server	1291
Accessing the tempdb database	1292
Analyzing database workload with Database Engine Tuning Advisor	1294
Collations and character sets	1296
Creating a database user	1299
Determining a recovery model	1300
Determining the last failover time	1300
Disabling fast inserts	1301
Dropping a SQL Server database	1301
Renaming a Multi-AZ database	1301
Resetting the db_owner role password	1302
Restoring license-terminated DB instances	1302
Transitioning a database from OFFLINE to ONLINE	1303
Using CDC	1303
Using SQL Server Agent	1305
Working with SQL Server logs	1308
Working with trace and dump files	1309
MySQL on Amazon RDS	1310
MySQL feature support	1312
Supported storage engines	1312
Using memcached and other options	1312
InnoDB cache warming	1313
Features not supported	1313
MySQL versions	1315
Supported MySQL versions	1315
MySQL release calendar	1316
Deprecated MySQL versions	1317
Connecting to a DB instance running MySQL	1318
Finding the connection information	1319
Connecting from the MySQL command-line client (unencrypted)	1321
Connecting from MySQL Workbench	1322
Connecting with the AWS JDBC Driver for MySQL	1323
Troubleshooting	1324
Securing MySQL connections	1325
MySQL security	1325
Password Validation Plugin	1326
Encrypting with SSL/TLS	1327
Using new SSL/TLS certificates	1330

Using Kerberos authentication for MySQL	1333
Upgrading the MySQL DB engine	1343
Overview	1343
Major version upgrades	1344
Testing an upgrade	1348
Upgrading a MySQL DB instance	1348
Automatic minor version upgrades	1348
Upgrading with reduced downtime	1350
Upgrading a MySQL DB snapshot	1353
Importing data into a MySQL DB instance	1355
Overview	1355
Importing data considerations	1357
Restoring a backup into a MySQL DB instance	1361
Importing data from an external database	1369
Importing data to a DB instance with reduced downtime	1371
Importing data from any source	1384
Working with MySQL replication	1389
Working with MySQL read replicas	1389
Using GTID-based replication	1401
Configuring GTID-based replication with an external source instance	1405
Configuring binary log file position replication with an external source instance	1408
Exporting data from a MySQL DB instance	1412
Prepare an external MySQL database	1412
Prepare the source MySQL DB instance	1413
Copy the database	1414
Complete the export	1414
Options for MySQL	1416
MariaDB Audit Plugin	1417
memcached	1422
Parameters for MySQL	1426
Common DBA tasks for MySQL	1428
Ending a session or query	1428
Skipping the current replication error	1428
Working with InnoDB tablespaces to improve crash recovery times	1429
Managing the global status history	1431
Local time zone	1433
Known issues and limitations	1435
InnoDB reserved word	1435
Storage-full behavior	1435
Inconsistent InnoDB buffer pool size	1436
Index merge optimization returns incorrect results	1436
Log file size	1437
MySQL parameter exceptions for Amazon RDS DB instances	1437
MySQL file size limits in Amazon RDS	1437
MySQL Keyring Plugin not supported	1438
MySQL on Amazon RDS SQL reference	1439
Overview	1439
SQL reference conventions	1440
mysql.rds_set_master_auto_position	1440
mysql.rds_set_external_master	1441
mysql.rds_set_external_master_with_delay	1443
mysql.rds_set_external_master_with_auto_position	1446
mysql.rds_reset_external_master	1448
mysql.rds_import_binlog_ssl_material	1449
mysql.rds_remove_binlog_ssl_material	1451
mysql.rds_set_source_delay	1451
mysql.rds_start_replication	1452

mysql.rds_start_replication_until	1452
mysql.rds_start_replication_until_gtid	1453
mysql.rds_stop_replication	1454
mysql.rds_skip_transaction_with_gtid	1455
mysql.rds_skip_repl_error	1455
mysql.rds_next_master_log	1456
mysql.rds_innodb_buffer_pool_dump_now	1458
mysql.rds_innodb_buffer_pool_load_now	1458
mysql.rds_innodb_buffer_pool_load_abort	1459
mysql.rds_set_configuration	1459
mysql.rds_show_configuration	1460
mysql.rds_kill	1461
mysql.rds_kill_query	1461
mysql.rds_rotate_general_log	1462
mysql.rds_rotate_slow_log	1462
mysql.rds_enable_gsh_collector	1463
mysql.rds_set_gsh_collector	1463
mysql.rds_disable_gsh_collector	1463
mysql.rds_collect_global_status_history	1463
mysql.rds_enable_gsh_rotation	1464
mysql.rds_set_gsh_rotation	1464
mysql.rds_disable_gsh_rotation	1464
mysql.rds_rotate_global_status_history	1464
Oracle on Amazon RDS	1466
Oracle overview	1467
Oracle features	1467
Oracle versions	1470
Oracle licensing	1474
Oracle instance classes	1477
Oracle architecture	1480
Oracle parameters	1482
Oracle character sets	1482
Oracle limitations	1485
Connecting to an Oracle instance	1488
Finding the endpoint	1488
SQL developer	1490
SQL*Plus	1492
Security group considerations	1493
Dedicated and shared server processes	1493
Troubleshooting	1493
Modifying Oracle sqlnet.ora parameters	1494
Securing Oracle connections	1498
Encrypting with SSL	1498
Using new SSL/TLS certificates	1498
Configuring Kerberos authentication	1501
Configuring UTL_HTTP access	1513
Administering your Oracle DB	1521
System tasks	1529
Database tasks	1543
Log tasks	1560
RMAN tasks	1568
Oracle Scheduler tasks	1585
Diagnostic tasks	1590
Other tasks	1597
Configuring advanced RDS for Oracle features	1604
Configuring the instance store	1604
Turning on HugePages	1610

Turning on extended data types	1613
Importing data into Oracle	1615
Importing using Oracle SQL Developer	1615
Importing using Oracle Data Pump	1616
Importing using Oracle Export/Import	1626
Importing using Oracle SQL*Loader	1627
Migrating with Oracle materialized views	1628
Working with Oracle replicas	1630
Overview of Oracle replicas	1630
Considerations for Oracle replicas	1631
Preparing to create an Oracle replica	1633
Creating a mounted Oracle replica	1634
Modifying the replica mode	1636
Working with Oracle replica backups	1636
Performing an Oracle Data Guard switchover	1638
Troubleshooting Oracle replicas	1644
Options for Oracle	1646
Overview of Oracle DB options	1646
Amazon S3 integration	1648
Application Express (APEX)	1664
Amazon EFS integration	1675
Java virtual machine (JVM)	1685
Enterprise Manager	1688
Label security	1703
Locator	1706
Multimedia	1709
Native network encryption (NNE)	1711
OLAP	1719
Secure Sockets Layer (SSL)	1722
Spatial	1730
SQLT	1733
Statspack	1739
Time zone	1742
Time zone file autoupgrade	1746
Transparent Data Encryption (TDE)	1751
UTL_MAIL	1753
XML DB	1756
Upgrading the Oracle DB engine	1757
Overview of Oracle upgrades	1757
Major version upgrades	1759
Minor version upgrades	1760
Upgrade considerations	1761
Testing an upgrade	1763
Upgrading an Oracle DB instance	1764
Upgrading an Oracle DB snapshot	1764
Tools and third-party software for Oracle	1766
Setting up	1767
Using Oracle GoldenGate	1773
Using the Oracle Repository Creation Utility	1786
Configuring CMAN	1792
Installing a Siebel database on Oracle on Amazon RDS	1794
Oracle Database engine releases	1797
PostgreSQL on Amazon RDS	1798
Common management tasks	1799
The database preview environment	1802
Features not supported in the preview environment	1802
Creating a new DB instance in the preview environment	1802

PostgreSQL version 15 in the database preview environment	1804
PostgreSQL versions	1805
Deprecation of PostgreSQL version 10	1805
Deprecation of PostgreSQL version 9.6	1806
Deprecated PostgreSQL versions	1806
PostgreSQL extension versions	1807
Restricting installation of PostgreSQL extensions	1807
PostgreSQL trusted extensions	1808
Connecting to a PostgreSQL instance	1809
Using pgAdmin to connect to a RDS for PostgreSQL DB instance	1811
Using psql to connect to your RDS for PostgreSQL DB instance	1813
Connecting with the AWS JDBC Driver for PostgreSQL	1813
Troubleshooting connections to your RDS for PostgreSQL instance	1814
Securing connections with SSL/TLS	1816
Using SSL with a PostgreSQL DB instance	1816
Updating applications to use new SSL/TLS certificates	1819
Using Kerberos authentication	1823
Region and version availability	1823
Overview of Kerberos authentication	1823
Setting up	1824
Managing a DB instance in a Domain	1833
Connecting with Kerberos authentication	1834
Using a custom DNS server for outbound network access	1837
Turning on custom DNS resolution	1837
Turning off custom DNS resolution	1837
Setting up a custom DNS server	1837
Upgrading the PostgreSQL DB engine	1839
Overview of upgrading	1840
PostgreSQL version numbers	1841
Choosing a major version upgrade	1841
How to perform a major version upgrade	1843
Automatic minor version upgrades	1847
Upgrading PostgreSQL extensions	1849
Upgrading a PostgreSQL DB snapshot engine version	1850
Working with read replicas for RDS for PostgreSQL	1852
Read replica limitations with PostgreSQL	1852
Read replica configuration with PostgreSQL	1853
How replication works for different RDS for PostgreSQL versions	1855
Monitoring and tuning the replication process	1857
Importing data into PostgreSQL	1860
Importing a PostgreSQL database from an Amazon EC2 instance	1861
Using the \copy command to import data to a table on a PostgreSQL DB instance	1863
Importing data from Amazon S3 into RDS for PostgreSQL	1864
Transporting PostgreSQL databases between DB instances	1877
Exporting PostgreSQL data to Amazon S3	1883
Installing the extension	1883
Overview of exporting to S3	1884
Specifying the Amazon S3 file path to export to	1885
Setting up access to an Amazon S3 bucket	1886
Exporting query data using the aws_s3.query_export_to_s3 function	1889
Troubleshooting access to Amazon S3	1891
Function reference	1891
Invoking a Lambda function from RDS for PostgreSQL	1895
Step 1: Configure outbound connections	1895
Step 2: Configure IAM for your instance and Lambda	1896
Step 3: Install the extension	1897
Step 4: Use Lambda helper functions	1898

Step 5: Invoke a Lambda function	1898
Step 6: Grant users permissions	1899
Examples: Invoking Lambda functions	1900
Lambda function error messages	1902
Lambda function reference	1903
PostgreSQL features	1905
Custom data types and enumerations	1906
Event triggers for RDS for PostgreSQL	1907
Huge pages for RDS for PostgreSQL	1907
Logical replication	1908
RAM disk for the stats_temp_directory	1909
Tablespaces for RDS for PostgreSQL	1910
RDS for PostgreSQL collations for EBCDIC and other mainframe migrations	1910
Common DBA tasks for RDS for PostgreSQL	1915
Understanding PostgreSQL roles and permissions	1915
Working with the PostgreSQL autovacuum	1924
Logging mechanisms	1933
Using pgBadger for log analysis with PostgreSQL	1933
Working with parameters	1934
Using PostgreSQL extensions	1945
Using functions from orafce	1946
Managing partitions with the pg_partman extension	1947
Using pgAudit to log database activity	1951
Scheduling maintenance with the pg_cron extension	1960
Using pglogical to synchronize data	1967
Reducing bloat with the pg_repack extension	1977
Upgrading and using PLV8	1978
Managing spatial data with PostGIS	1980
Supported foreign data wrappers	1987
Using the log_fdw extension	1987
Using postgres_fdw to access external data	1988
Working with a MySQL database	1989
Working with an Oracle database	1992
Working with a SQL Server database	1995
Security	1997
Database authentication	1998
Password authentication	1998
IAM database authentication	1999
Kerberos authentication	1999
Data protection	1999
Data encryption	2000
Internetwork traffic privacy	2015
Identity and access management	2016
Audience	2016
Authenticating with identities	2016
Managing access using policies	2018
How Amazon RDS works with IAM	2020
Identity-based policy examples	2025
AWS managed policies	2036
Policy updates	2043
Cross-service confused deputy prevention	2046
IAM database authentication	2048
Troubleshooting	2075
Logging and monitoring	2077
Compliance validation	2079
Resilience	2080
Backup and restore	2080

Replication	2080
Failover	2080
Infrastructure security	2081
Security groups	2081
Public accessibility	2081
VPC endpoints (AWS PrivateLink)	2082
Considerations	2082
Availability	2082
Creating an interface VPC endpoint	2083
Creating a VPC endpoint policy	2083
Security best practices	2084
Controlling access with security groups	2085
Overview of VPC security groups	2085
Security group scenario	2085
Creating a VPC security group	2086
Associating with a DB instance	2087
Master user account privileges	2087
Service-linked roles	2089
Service-linked role permissions for Amazon RDS	2089
Service-linked role permissions for Amazon RDS Custom	2093
Using Amazon RDS with Amazon VPC	2103
Working with a DB instance in a VPC	2103
Updating the VPC for a DB instance	2114
Scenarios for accessing a DB instance in a VPC	2115
Tutorial: Create a VPC for use with a DB instance (IPv4 only)	2120
Tutorial: Create a VPC for use with a DB instance (dual-stack mode)	2126
Moving a DB instance into a VPC	2133
Quotas and constraints	2135
Quotas in Amazon RDS	2135
Naming constraints in Amazon RDS	2138
Maximum number of database connections	2139
File size limits in Amazon RDS	2140
Troubleshooting	2141
Can't connect to DB instance	2141
Testing the DB instance connection	2142
Troubleshooting connection authentication	2143
Security issues	2143
Error message "failed to retrieve account attributes, certain console functions may be impaired."	2143
Resetting the DB instance owner password	2144
DB instance outage or reboot	2144
Parameter changes not taking effect	2144
DB instance out of storage	2145
Insufficient DB instance capacity	2146
RDS freeable memory issues	2146
MySQL and MariaDB issues	2147
Maximum MySQL and MariaDB connections	2147
Diagnosing and resolving incompatible parameters status for a memory limit	2148
Diagnosing and resolving lag between read replicas	2149
Diagnosing and resolving a MySQL or MariaDB read replication failure	2150
Creating triggers with binary logging enabled requires SUPER privilege	2151
Diagnosing and resolving point-in-time restore failures	2152
Replication stopped error	2153
Read replica create fails or replication breaks with fatal error 1236	2153
Can't set backup retention period to 0	2154
Amazon RDS API reference	2155
Using the Query API	2155

Query parameters	2155
Query request authentication	2155
Troubleshooting applications	2155
Retrieving errors	2156
Troubleshooting tips	2156
Document history	2157
Earlier updates	2210
AWS glossary	2228

What is Amazon Relational Database Service (Amazon RDS)?

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

Note

This guide covers Amazon RDS database engines other than Amazon Aurora. For information about using Amazon Aurora, see the [Amazon Aurora User Guide](#).

If you are new to AWS products and services, begin learning more with the following resources:

- For an overview of all AWS products, see [What is cloud computing?](#)
- Amazon Web Services provides a number of database services. For guidance on which service is best for your environment, see [Running databases on AWS](#).

Overview of Amazon RDS

Why do you want to run a relational database in the AWS Cloud? Because AWS takes over many of the difficult and tedious management tasks of a relational database.

Topics

- [Amazon EC2 and on-premises databases \(p. 1\)](#)
- [Amazon RDS and Amazon EC2 \(p. 2\)](#)
- [Amazon RDS Custom for Oracle and Microsoft SQL Server \(p. 3\)](#)
- [Amazon RDS on AWS Outposts \(p. 3\)](#)

Amazon EC2 and on-premises databases

Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the AWS Cloud. Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.

When you buy an on-premises server, you get CPU, memory, storage, and IOPS, all bundled together. With Amazon EC2, these are split apart so that you can scale them independently. If you need more CPU, less IOPS, or more storage, you can easily allocate them.

For a relational database in an on-premises server, you assume full responsibility for the server, operating system, and software. For a database on an Amazon EC2 instance, AWS manages the layers below the operating system. In this way, Amazon EC2 eliminates some of the burden of managing an on-premises database server.

In the following table, you can find a comparison of the management models for on-premises databases and Amazon EC2.

Feature	On-premises management	Amazon EC2 management
Application optimization	Customer	Customer
Scaling	Customer	Customer
High availability	Customer	Customer
Database backups	Customer	Customer
Database software patching	Customer	Customer
Database software install	Customer	Customer
Operating system (OS) patching	Customer	Customer
OS installation	Customer	Customer
Server maintenance	Customer	AWS
Hardware lifecycle	Customer	AWS
Power, network, and cooling	Customer	AWS

Amazon EC2 isn't a fully managed service. Thus, when you run a database on Amazon EC2, you're more prone to user errors. For example, when you update the operating system or database software manually, you might accidentally cause application downtime. You might spend hours checking every change to identify and fix an issue.

Amazon RDS and Amazon EC2

Amazon RDS is a managed database service. It's responsible for most management tasks. By eliminating tedious manual tasks, Amazon RDS frees you to focus on your application and your users. We recommend Amazon RDS over Amazon EC2 as your default choice for most database deployments.

In the following table, you can find a comparison of the management models in Amazon EC2 and Amazon RDS.

Feature	Amazon EC2 management	Amazon RDS management
Application optimization	Customer	Customer
Scaling	Customer	AWS
High availability	Customer	AWS
Database backups	Customer	AWS
Database software patching	Customer	AWS
Database software install	Customer	AWS
OS patching	Customer	AWS
OS installation	Customer	AWS
Server maintenance	AWS	AWS
Hardware lifecycle	AWS	AWS

Feature	Amazon EC2 management	Amazon RDS management
Power, network, and cooling	AWS	AWS

Amazon RDS provides the following specific advantages over database deployments that aren't fully managed:

- You can use the database products you are already familiar with: MariaDB, Microsoft SQL Server, MySQL, Oracle, and PostgreSQL.
- Amazon RDS manages backups, software patching, automatic failure detection, and recovery.
- You can turn on automated backups, or manually create your own backup snapshots. You can use these backups to restore a database. The Amazon RDS restore process works reliably and efficiently.
- You can get high availability with a primary instance and a synchronous secondary instance that you can fail over to when problems occur. You can also use read replicas to increase read scaling.
- In addition to the security in your database package, you can help control who can access your RDS databases. To do so, you can use AWS Identity and Access Management (IAM) to define users and permissions. You can also help protect your databases by putting them in a virtual private cloud (VPC).

Amazon RDS Custom for Oracle and Microsoft SQL Server

Amazon RDS Custom is an RDS management type that gives you full access to your database and operating system.

You can use the control capabilities of RDS Custom to access and customize the database environment and operating system for legacy and packaged business applications. Meanwhile, Amazon RDS automates database administration tasks and operations.

In this deployment model, you can install applications and change configuration settings to suit your applications. At the same time, you can offload database administration tasks such as provisioning, scaling, upgrading, and backup to AWS. You can take advantage of the database management benefits of Amazon RDS, with more control and flexibility.

For Oracle Database and Microsoft SQL Server, RDS Custom combines the automation of Amazon RDS with the flexibility of Amazon EC2. For more information on RDS Custom, see [Working with Amazon RDS Custom \(p. 755\)](#).

With the shared responsibility model of RDS Custom, you get more control than in Amazon RDS, but also more responsibility. For more information, see [Shared responsibility model \(p. 756\)](#).

Amazon RDS on AWS Outposts

Amazon RDS on AWS Outposts extends RDS for SQL Server, RDS for MySQL, and RDS for PostgreSQL databases to AWS Outposts environments. AWS Outposts uses the same hardware as in public AWS Regions to bring AWS services, infrastructure, and operation models on-premises. With RDS on Outposts, you can provision managed DB instances close to the business applications that must run on-premises. For more information, see [Working with Amazon RDS on AWS Outposts \(p. 902\)](#).

DB instances

A *DB instance* is an isolated database environment in the AWS Cloud. The basic building block of Amazon RDS is the DB instance.

Your DB instance can contain one or more user-created databases. You can access your DB instance by using the same tools and applications that you use with a standalone database instance. You can create and modify a DB instance by using the AWS Command Line Interface (AWS CLI), the Amazon RDS API, or the AWS Management Console.

DB engines

A *DB engine* is the specific relational database software that runs on your DB instance. Amazon RDS currently supports the following engines:

- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

Each DB engine has its own supported features, and each version of a DB engine can include specific features. Support for Amazon RDS features varies across AWS Regions and specific versions of each DB engine. To check feature support in different engine versions and Regions, see [Supported features in Amazon RDS by AWS Region and DB engine \(p. 77\)](#).

Additionally, each DB engine has a set of parameters in a DB parameter group that control the behavior of the databases that it manages.

DB instance classes

A *DB instance class* determines the computation and memory capacity of a DB instance. A DB instance class consists of both the DB instance type and the size. Each instance type offers different compute, memory, and storage capabilities. For example, db.m6g is a general-purpose DB instance type powered by AWS Graviton2 processors. Within the db.m6g instance type, db.m6g.2xlarge is a DB instance class.

You can select the DB instance that best meets your needs. If your needs change over time, you can change DB instances. For information, see [DB instance classes \(p. 10\)](#).

Note

For pricing information on DB instance classes, see the Pricing section of the [Amazon RDS product page](#).

DB instance storage

Amazon EBS provides durable, block-level storage volumes that you can attach to a running instance. DB instance storage comes in the following types:

- General Purpose (SSD)
- Provisioned IOPS (PIOPS)
- Magnetic

The storage types differ in performance characteristics and price. You can tailor your storage performance and cost to the needs of your database.

Each DB instance has minimum and maximum storage requirements depending on the storage type and the database engine it supports. It's important to have sufficient storage so that your databases have room to grow. Also, sufficient storage makes sure that features for the DB engine have room to write content or log entries. For more information, see [Amazon RDS DB instance storage \(p. 64\)](#).

Amazon Virtual Private Cloud (Amazon VPC)

You can run a DB instance on a virtual private cloud (VPC) using the Amazon Virtual Private Cloud (Amazon VPC) service. When you use a VPC, you have control over your virtual networking environment. You can choose your own IP address range, create subnets, and configure routing and access control lists. The basic functionality of Amazon RDS is the same whether it's running in a VPC or not. Amazon RDS manages backups, software patching, automatic failure detection, and recovery. There's no additional cost to run your DB instance in a VPC. For more information on using Amazon VPC with RDS, see [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#).

Amazon RDS uses Network Time Protocol (NTP) to synchronize the time on DB Instances.

AWS Regions and Availability Zones

Amazon cloud computing resources are housed in highly available data center facilities in different areas of the world (for example, North America, Europe, or Asia). Each data center location is called an AWS Region.

Each AWS Region contains multiple distinct locations called Availability Zones, or AZs. Each Availability Zone is engineered to be isolated from failures in other Availability Zones. Each is engineered to provide inexpensive, low-latency network connectivity to other Availability Zones in the same AWS Region. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. For more information, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

You can run your DB instance in several Availability Zones, an option called a Multi-AZ deployment. When you choose this option, Amazon automatically provisions and maintains one or more secondary standby DB instances in a different Availability Zone. Your primary DB instance is replicated across Availability Zones to each secondary DB instance. This approach helps provide data redundancy and failover support, eliminate I/O freezes, and minimize latency spikes during system backups. In a Multi-AZ DB clusters deployment, the secondary DB instances can also serve read traffic. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Security

A *security group* controls the access to a DB instance. It does so by allowing access to IP address ranges or Amazon EC2 instances that you specify.

For more information about security groups, see [Security in Amazon RDS \(p. 1997\)](#).

Monitoring an Amazon RDS DB instance

There are several ways that you can track the performance and health of a DB instance. You can use the Amazon CloudWatch service to monitor the performance and health of a DB instance. CloudWatch performance charts are shown in the Amazon RDS console. You can also subscribe to Amazon RDS events to be notified about changes to a DB instance, DB snapshot, or DB parameter group. For more information, see [Monitoring metrics in an Amazon RDS instance \(p. 510\)](#).

How to work with Amazon RDS

There are several ways that you can interact with Amazon RDS.

AWS Management Console

The AWS Management Console is a simple web-based user interface. You can manage your DB instances from the console with no programming required. To access the Amazon RDS console, sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

Command line interface

You can use the AWS Command Line Interface (AWS CLI) to access the Amazon RDS API interactively. To install the AWS CLI, see [Installing the AWS Command Line Interface](#). To begin using the AWS CLI for RDS, see [AWS Command Line Interface reference for Amazon RDS](#).

Programming with Amazon RDS

If you are a developer, you can access the Amazon RDS programmatically. For more information, see [Amazon RDS API reference \(p. 2155\)](#).

For application development, we recommend that you use one of the AWS Software Development Kits (SDKs). The AWS SDKs handle low-level details such as authentication, retry logic, and error handling, so that you can focus on your application logic. AWS SDKs are available for a wide variety of languages. For more information, see [Tools for Amazon web services](#).

AWS also provides libraries, sample code, tutorials, and other resources to help you get started more easily. For more information, see [Sample code & libraries](#).

How you are charged for Amazon RDS

When you use Amazon RDS, you can choose to use on-demand DB instances or reserved DB instances. For more information, see [DB instance billing for Amazon RDS \(p. 138\)](#).

For Amazon RDS pricing information, see the [Amazon RDS product page](#).

What's next?

The preceding section introduced you to the basic infrastructure components that RDS offers. What should you do next?

Getting started

Create a DB instance using instructions in [Getting started with Amazon RDS \(p. 153\)](#).

Topics specific to database engines

You can review information specific to a particular DB engine in the following sections:

- [Amazon RDS for MariaDB \(p. 974\)](#)
- [Amazon RDS for Microsoft SQL Server \(p. 1058\)](#)
- [Amazon RDS for MySQL \(p. 1310\)](#)
- [Amazon RDS for Oracle \(p. 1466\)](#)
- [Amazon RDS for PostgreSQL \(p. 1798\)](#)

Amazon RDS DB instances

A *DB instance* is an isolated database environment running in the cloud. It is the basic building block of Amazon RDS. A DB instance can contain multiple user-created databases, and can be accessed using the same client tools and applications you might use to access a standalone database instance. DB instances are simple to create and modify with the AWS command line tools, Amazon RDS API operations, or the AWS Management Console.

Note

Amazon RDS supports access to databases using any standard SQL client application. Amazon RDS does not allow direct host access.

You can have up to 40 Amazon RDS DB instances, with the following limitations:

- 10 for each SQL Server edition (Enterprise, Standard, Web, and Express) under the "license-included" model
- 10 for Oracle under the "license-included" model
- 40 for MySQL, MariaDB, or PostgreSQL
- 40 for Oracle under the "bring-your-own-license" (BYOL) licensing model

Note

If your application requires more DB instances, you can request additional DB instances by using [this form](#).

Each DB instance has a DB instance identifier. This customer-supplied name uniquely identifies the DB instance when interacting with the Amazon RDS API and AWS CLI commands. The DB instance identifier must be unique for that customer in an AWS Region.

The identifier is used as part of the DNS hostname allocated to your instance by RDS. For example, if you specify db1 as the DB instance identifier, then RDS will automatically allocate a DNS endpoint for your instance, such as db1.123456789012.us-east-1.rds.amazonaws.com, where 123456789012 is the fixed identifier for a specific region for your account.

Each DB instance supports a database engine. Amazon RDS currently supports MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server, and Amazon Aurora database engines.

When creating a DB instance, some database engines require that a database name be specified. A DB instance can host multiple databases, or a single Oracle database with multiple schemas. The database name value depends on the database engine:

- For the MySQL and MariaDB database engines, the database name is the name of a database hosted in your DB instance. Databases hosted by the same DB instance must have a unique name within that instance.
- For the Oracle database engine, database name is used to set the value of ORACLE_SID, which must be supplied when connecting to the Oracle RDS instance.
- For the Microsoft SQL Server database engine, database name is not a supported parameter.
- For the PostgreSQL database engine, the database name is the name of a database hosted in your DB instance. A database name is not required when creating a DB instance. Databases hosted by the same DB instance must have a unique name within that instance.

Amazon RDS creates a master user account for your DB instance as part of the creation process. This master user has permissions to create databases and to perform create, delete, select, update, and insert operations on tables the master user creates. You must set the master user password when you create a DB instance, but you can change it at any time using the AWS CLI, Amazon RDS API operations, or the

AWS Management Console. You can also change the master user password and manage users using standard SQL commands.

Note

This guide covers non-Aurora Amazon RDS database engines. For information about using Amazon Aurora, see the [Amazon Aurora User Guide](#).

DB instance classes

The DB instance class determines the computation and memory capacity of an Amazon RDS DB instance. The DB instance class that you need depends on your processing power and memory requirements.

A DB instance class consists of both the DB instance type and the size. For example, db.m6g is a general-purpose DB instance type powered by AWS Graviton2 processors. Within the db.m6g instance type, db.m6g.2xlarge is a DB instance class.

For more information about instance class pricing, see [Amazon RDS pricing](#).

Topics

- [DB instance class types \(p. 10\)](#)
- [Supported DB engines for DB instance classes \(p. 12\)](#)
- [Determining DB instance class support in AWS Regions \(p. 39\)](#)
- [Changing your DB instance class \(p. 42\)](#)
- [Configuring the processor for a DB instance class \(p. 42\)](#)
- [Hardware specifications for DB instance classes \(p. 55\)](#)

DB instance class types

Amazon RDS supports three types of instance classes: general purpose, memory optimized, and burstable performance. For more information about Amazon EC2 instance types, see [Instance types](#) in the Amazon EC2 documentation.

The following are the general-purpose DB instance types available:

- **db.m6g** – General-purpose instance classes powered by AWS Graviton2 processors. These deliver balanced compute, memory, and networking for a broad range of general-purpose workloads.

You can modify a DB instance to use one of the DB instance classes powered by AWS Graviton2 processors. To do so, complete the same steps as with any other DB instance modification.

- **db.m6gd** – General-purpose instance classes powered by AWS Graviton2 processors. These deliver balanced compute, memory, and networking for a broad range of general-purpose workloads. These have local NVMe-based SSD block-level storage for applications that need high-speed, low latency local storage.

These DB instance classes are only supported for Multi-AZ DB clusters. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

- **db.m6i** – General-purpose instance classes that are well suited for a broad range of general-purpose workloads.
- **db.m5d** – General-purpose instance classes that are optimized for low latency, very high random I/O performance, and high sequential read throughput.

For the RDS for MySQL and RDS for PostgreSQL DB engines, these DB instance classes are only supported for Multi-AZ DB clusters. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

- **db.m5** – General-purpose instance classes that provide a balance of compute, memory, and network resources, and are a good choice for many applications. The db.m5 instance classes provide more computing capacity than the previous db.m4 instance classes. They are powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor.
- **db.m4** – General-purpose instance classes that provide more computing capacity than the previous db.m3 instance classes.

- **db.m3** – General-purpose instance classes that provide more computing capacity than the previous db.m1 instance classes.

Amazon RDS has started the end-of-life process for db.m3 DB instance classes using the following schedule, which includes upgrade recommendations. For all RDS DB instances that use db.m3 DB instance classes, we recommend that you upgrade to a db.m5 DB instance class as soon as possible.

Action or recommendation	Dates
We recommend that you manually upgrade db.m3 DB instance classes to db.m5 DB instance classes for your RDS DB instances.	Now–February 1, 2023
You can no longer create RDS DB instances that use db.m3 DB instance classes.	Now
Amazon RDS starts automatic upgrades of RDS DB instances that use db.m3 DB instance classes to equivalent db.m5 DB instance classes.	February 1, 2023

The following are the memory optimized DB instance types available:

- **db.x2g** – Instance classes optimized for memory-intensive applications and powered by AWS Graviton2 processors. These offer low cost per GiB of memory.

You can modify a DB instance to use one of the DB instance classes powered by AWS Graviton2 processors. To do so, complete the same steps as with any other DB instance modification.
- **db.z1d** – Instance classes optimized for memory-intensive applications. These offer both high compute capacity and a high memory footprint. High frequency z1d instances deliver a sustained all core frequency of up to 4.0 GHz.
- **db.x1e** – Instance classes optimized for memory-intensive applications. These offer one of the lowest price per gibibyte (GiB) of RAM among the DB instance classes and up to 3,904 GiB of DRAM-based instance memory.
- **db.x1** – Instance classes optimized for memory-intensive applications. These offer one of the lowest price per GiB of RAM among the DB instance classes and up to 1,952 GiB of DRAM-based instance memory.
- **db.r6g** – Instance classes powered by AWS Graviton2 processors. These are ideal for running memory-intensive workloads in open-source databases such as MySQL and PostgreSQL.

You can modify a DB instance to use one of the DB instance classes powered by AWS Graviton2 processors. To do so, complete the same steps as with any other DB instance modification.

- **db.r6gd** – Instance classes powered by AWS Graviton2 processors. These are ideal for running memory-intensive workloads in open-source databases such as MySQL and PostgreSQL. These have local NVMe-based SSD block-level storage for applications that need high-speed, low latency local storage.

These DB instance classes are only supported for Multi-AZ DB clusters. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

- **db.r6i** – Instance classes that are ideal for running memory-intensive workloads.
- **db.r5b** – Instance classes that are memory optimized for throughput-intensive applications. Powered by the AWS Nitro System, db.r5b instances deliver up to 60 Gbps bandwidth and 260,000 IOPS of EBS performance. This is the fastest block storage performance on EC2.
- **db.r5d** – Instance classes that are optimized for low latency, very high random I/O performance, and high sequential read throughput.

For the RDS for MySQL and RDS for PostgreSQL DB engines, these DB instance classes are only supported for Multi-AZ DB clusters. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

- **db.r5** – Instance classes optimized for memory-intensive applications. These offer improved networking and Amazon Elastic Block Store (Amazon EBS) performance. They are powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor.
- **db.r3** – Instance classes that provide memory optimization.

Amazon RDS has started the end-of-life process for db.r3 DB instance classes using the following schedule, which includes upgrade recommendations. For all RDS DB instances that use db.r3 DB instance classes, we recommend that you upgrade to a db.r5 DB instance class as soon as possible.

Action or recommendation	Dates
We recommend that you manually upgrade db.r3 DB instance classes to db.r5 DB instance classes for your RDS DB instances.	Now–February 1, 2023
You can no longer create RDS DB instances that use db.r3 DB instance classes.	Now
Amazon RDS starts automatic upgrades of RDS DB instances that use db.r3 DB instance classes to equivalent db.r5 DB instance classes.	February 1, 2023

The following are the burstable-performance DB instance types available:

- **db.t4g** – General-purpose instance classes powered by Arm-based AWS Graviton2 processors. These deliver better price performance than previous burstable-performance DB instance classes for a broad set of burstable general-purpose workloads. Amazon RDS T4g instances are configured for Unlimited mode. This means that they can burst beyond the baseline over a 24-hour window for an additional charge.

You can modify a DB instance to use one of the DB instance classes powered by AWS Graviton2 processors. To do so, complete the same steps as with any other DB instance modification.

- **db.t3** – Instance classes that provide a baseline performance level, with the ability to burst to full CPU usage. T3 instances are configured for Unlimited mode. These instance classes provide more computing capacity than the previous db.t2 instance classes. They are powered by the AWS Nitro System, a combination of dedicated hardware and lightweight hypervisor.
- **db.t2** – Instance classes that provide a baseline performance level, with the ability to burst to full CPU usage. T2 instances can be configured for Unlimited mode. We recommend using these instance classes only for development and test servers, or other nonproduction servers.

Note

The DB instance classes that use the AWS Nitro System (db.m5, db.r5, db.t3) are throttled on combined read plus write workload.

For DB instance class hardware specifications, see [Hardware specifications for DB instance classes \(p. 55\)](#).

Supported DB engines for DB instance classes

The following are DB engine-specific considerations for DB instance classes:

Microsoft SQL Server

DB instance class support varies according to the version and edition of SQL Server. For instance class support by version and edition, see [DB instance class support for Microsoft SQL Server \(p. 1062\)](#).

Oracle

DB instance class support varies according to the Oracle Database version and edition. RDS for Oracle supports additional memory-optimized instance classes. These classes have names of the form db.r5.*instance_size*.tpc*threads_per_core*.mem*ratio*. For the vCPU count and memory allocation for each optimized class, see [Supported RDS for Oracle instance classes \(p. 1477\)](#).

In the following table, you can find details about supported Amazon RDS DB instance classes for each Amazon RDS DB engine.

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6g – general-purpose instance classes powered by AWS Graviton2 processors					
db.m6g.16xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6g.12xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6g.8xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6g.4xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
					12.7 and higher
db.m6g.2xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6g.xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6g.large	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.m6gd – general-purpose instance classes powered by AWS Graviton2 processors					
db.m6gd.16xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6gd.12xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6gd.8xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6gd.4xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6gd.2xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6gd.xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6gd.large	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.m6i – general-purpose instance classes					
db.m6i.32xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m6i.24xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.16xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m6i.12xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m6i.8xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.4xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m6i.2xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m6i.xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.large	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Oracle Database 19c	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.m5d – general-purpose instance classes					
db.m5d.24xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.16xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.12xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.8xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.4xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.2xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5d.xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5d.large	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.m5 – general-purpose instance classes					
db.m5.24xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.16xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.12xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.8xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.4xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5.2xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m5.large	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.m4 – general-purpose instance classes					
db.m4.16xlarge	Yes	Yes	MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.m4.10xlarge	Yes	Yes	Yes	Yes	Lower than PostgreSQL 13
db.m4.4xlarge	Yes	Yes	Yes	Yes	Lower than PostgreSQL 13
db.m4.2xlarge	Yes	Yes	Yes	Yes	Lower than PostgreSQL 13
db.m4.xlarge	Yes	Yes	Yes	Yes	Lower than PostgreSQL 13
db.m4.large	Yes	Yes	Yes	Yes	Lower than PostgreSQL 13
db.m3 – general-purpose instance classes					

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m3.2xlarge	No	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.m3.xlarge	No	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.m3.large	No	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.m3.medium	No	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.x2g – memory-optimized instance classes powered by AWS Graviton2 processors					
db.x2g.16xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.x2g.12xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.x2g.8xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x2g.4xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.x2g.2xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.x2g.xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.x2g.large	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.z1d – memory-optimized instance classes					
db.z1d.12xlarge	No	Yes	No	Yes	No
db.z1d.6xlarge	No	Yes	No	Yes	No
db.z1d.3xlarge	No	Yes	No	Yes	No
db.z1d.2xlarge	No	Yes	No	Yes	No
db.z1d.xlarge	No	Yes	No	Yes	No
db.z1d.large	No	Yes	No	Yes	No
db.x1e – memory-optimized instance classes					

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x1e.32xlarge	No	Yes	No	Yes	No
db.x1e.16xlarge	No	Yes	No	Yes	No
db.x1e.8xlarge	No	Yes	No	Yes	No
db.x1e.4xlarge	No	Yes	No	Yes	No
db.x1e.2xlarge	No	Yes	No	Yes	No
db.x1e.xlarge	No	Yes	No	Yes	No
db.x1 – memory-optimized instance classes					
db.x1.32xlarge	No	Yes	No	Yes	No
db.x1.16xlarge	No	Yes	No	Yes	No
db.r6g – memory-optimized instance classes powered by AWS Graviton2 processors					
db.r6g.16xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6g.12xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6g.8xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6g.4xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6g.2xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6g.xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6g.large	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.23 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r6gd – memory-optimized instance classes powered by AWS Graviton2 processors					
db.r6gd.16xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6gd.12xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6gd.8xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6gd.4xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6gd.2xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6gd.xlarge	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6gd.large	No	No	MySQL 8.0.28 & higher Multi-AZ DB clusters	No	PostgreSQL 13.4 Multi-AZ DB clusters
db.r6i – memory-optimized instance classes					
db.r6i.32xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6i.24xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r6i.16xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r6i.12xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6i.8xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r6i.4xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r6i.2xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6i.xlarge	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r6i.large	MariaDB version 10.6.7 & higher 10.6 versions, MariaDB version 10.5.15 & higher 10.5 versions, and MariaDB version 10.4.24 & higher 10.4 versions	Yes	MySQL version 8.0.28 & higher 8.0 versions	Yes	All PostgreSQL 14 versions; PostgreSQL 13.4, 12.8, 11.13 and higher
db.r5d – memory-optimized instance classes					
db.r5d.24xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.16xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.12xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.8xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5d.4xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.2xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.xlarge	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5d.large	No	Yes	MySQL 8.0.28 & higher Multi-AZ DB clusters	Yes	PostgreSQL 13.4 Multi-AZ DB clusters
db.r5b – memory-optimized instance classes preconfigured for high memory, storage, and I/O					
db.r5b.8xlarge(tpc2.mem3x)	No	No	No	Yes	No
db.r5b.6xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5b.4xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5b.4xlarge(tpc2.mem3x)	No	No	No	Yes	No
db.r5b.4xlarge(tpc2.mem2x)	No	No	No	Yes	No
db.r5b.2xlarge(tpc2.mem8x)	No	No	No	Yes	No
db.r5b.2xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5b.2xlarge(tpc1.mem2x)	No	No	No	Yes	No
db.r5b.xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5b.xlarge(tpc2.mem2x)	No	No	No	Yes	No
db.r5b.large(tpc1.mem2x)	No	No	No	Yes	No
db.r5b – memory-optimized instance classes					

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.24xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r5b.16xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.12xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r5b.8xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	>Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.4xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r5b.2xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.xlarge	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r5b.large	MariaDB version 10.6.5 & higher 10.6 versions, MariaDB version 10.5.12 & higher 10.5 versions, MariaDB version 10.4.24 & higher 10.4 versions, and MariaDB version 10.3.34 & higher 10.3 versions	Yes	MySQL 8.0.25 & higher	Yes	All PostgreSQL 14 versions, all PostgreSQL 13 versions; PostgreSQL 12.7 and higher
db.r5 – memory-optimized instance classes preconfigured for high memory, storage, and I/O					
db.r5.12xlarge(tpc2.mem2x)	No	No	No	Yes	No
db.r5.8xlarge(tpc2.mem3x)	No	No	No	Yes	No
db.r5.6xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5.4xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5.4xlarge(tpc2.mem3x)	No	No	No	Yes	No
db.r5.4xlarge(tpc2.mem2x)	No	No	No	Yes	No
db.r5.2xlarge(tpc2.mem8x)	No	No	No	Yes	No

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.2xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5.2xlarge(tpc1.mem2x)	No	No	No	Yes	No
db.r5.xlarge(tpc2.mem4x)	No	No	No	Yes	No
db.r5.xlarge(tpc2.mem2x)	No	No	No	Yes	No
db.r5.large(tpc1.mem2x)	No	No	No	Yes	No
db.r5 – memory-optimized instance classes					
db.r5.24xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.16xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.12xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.8xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.4xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.2xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r5.large	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, and 11 versions; 10.17 and higher; 9.6.22 and higher
db.r4 – memory-optimized instance classes					
db.r4.16xlarge	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r4.8xlarge	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r4.4xlarge	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r4.2xlarge	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r4.xlarge	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r4.large	Yes	Yes	All MySQL 8.0, 5.7	Yes	Lower than PostgreSQL 13
db.r3 – memory-optimized instance classes					

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r3.8xlarge**	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.r3.4xlarge	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.r3.2xlarge	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.r3.xlarge	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.r3.large	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.t4g – burstable-performance instance classes powered by AWS Graviton2 processors					
db.t4g.2xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.t4g.xlarge	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.t4g.large	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.t4g.medium	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 & 13 versions, and PostgreSQL 12.7 & higher 12 versions
db.t4g.small	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.t4g.micro	All MariaDB 10.6 versions, all MariaDB 10.5 versions, and all MariaDB 10.4 versions	No	MySQL 8.0.25 & higher	No	All PostgreSQL 14 versions, all PostgreSQL 13 versions, PostgreSQL 12.7 and higher
db.t3 – burstable-performance instance classes					
db.t3.2xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, 11, and 10 versions; PostgreSQL 9.6.22 & higher versions
db.t3.xlarge	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, 11, and 10 versions; PostgreSQL 9.6.22 & higher versions

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.t3.large	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, 11, and 10 versions, and PostgreSQL 9.6.22 & higher versions
db.t3.medium	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, 11, and 10 versions; PostgreSQL 9.6.22 & higher versions
db.t3.small	Yes	Yes	Yes	Yes	All PostgreSQL 14, 13, 12, 11, and 10 versions; PostgreSQL 9.6.22 & higher versions
db.t3.micro	Yes	No	Yes	Only on Oracle Database 12c Release 1 (12.1.0.2), which is deprecated	All PostgreSQL 14, 13, 12, 11, and 10 versions; PostgreSQL 9.6.22 & higher versions
db.t2 – burstable-performance instance classes					
db.t2.2xlarge	Yes	No	All MySQL 8.0, 5.7	Deprecated	Lower than PostgreSQL 13
db.t2.xlarge	Yes	No	All MySQL 8.0, 5.7	Deprecated	Lower than PostgreSQL 13
db.t2.large	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13

Instance class	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.t2.medium	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.t2.small	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13
db.t2.micro	Yes	Yes	Yes	Deprecated	Lower than PostgreSQL 13

Determining DB instance class support in AWS Regions

To determine the DB instance classes supported by each DB engine in a specific AWS Region, you can take one of several approaches. You can use the AWS Management Console, the [Amazon RDS Pricing](#) page, or the `describe-orderable-db-instance-options` command for the AWS Command Line Interface (AWS CLI).

Note

When you perform operations with the AWS CLI, it automatically shows the supported DB instance classes for a specific DB engine, DB engine version, and AWS Region. Examples of the operations that you can perform include creating and modifying a DB instance.

Contents

- [Using the Amazon RDS pricing page to determine DB instance class support in AWS Regions \(p. 39\)](#)
- [Using the AWS CLI to determine DB instance class support in AWS Regions \(p. 40\)](#)
 - [Listing the DB instance classes that are supported by a specific DB engine version in an AWS Region \(p. 40\)](#)
 - [Listing the DB engine versions that support a specific DB instance class in an AWS Region \(p. 41\)](#)

Using the Amazon RDS pricing page to determine DB instance class support in AWS Regions

You can use the [Amazon RDS Pricing](#) page to determine the DB instance classes supported by each DB engine in a specific AWS Region.

To use the pricing page to determine the DB instance classes supported by each engine in a Region

1. Go to [Amazon RDS Pricing](#).
2. Choose a DB engine.
3. On the pricing page for the DB engine, choose **On-Demand DB Instances** or **Reserved DB Instances**.
4. To see the DB instance classes available in an AWS Region, choose the AWS Region in **Region**.

Other choices might be available for some DB engines, such as **Single-AZ Deployment** or **Multi-AZ Deployment**.

Using the AWS CLI to determine DB instance class support in AWS Regions

You can use the AWS CLI to determine which DB instance classes are supported for specific DB engines and DB engine versions in an AWS Region. The following table shows the valid DB engine values.

Engine names	Engine values in CLI commands	More information about versions
MariaDB	mariadb	MariaDB on Amazon RDS versions (p. 982)
Microsoft SQL Server	sqlserver-ee sqlserver-se sqlserver-ex sqlserver-web	Microsoft SQL Server versions on Amazon RDS (p. 1066)
MySQL	mysql	MySQL on Amazon RDS versions (p. 1315)
Oracle	oracle-ee oracle-se2 oracle-se	Amazon RDS for Oracle Release Notes
PostgreSQL	postgres	Available PostgreSQL database versions (p. 1805)

For information about AWS Region names, see [AWS Regions \(p. 73\)](#).

The following examples demonstrate how to determine DB instance class support in an AWS Region using the [describe-orderable-db-instance-options](#) AWS CLI command.

Note

To limit the output, these examples show results only for the General Purpose SSD (gp2) storage type. If necessary, you can change the storage type to General Purpose SSD (gp3), Provisioned IOPS (io1), or magnetic (standard) in the commands.

Topics

- [Listing the DB instance classes that are supported by a specific DB engine version in an AWS Region \(p. 40\)](#)
- [Listing the DB engine versions that support a specific DB instance class in an AWS Region \(p. 41\)](#)

Listing the DB instance classes that are supported by a specific DB engine version in an AWS Region

To list the DB instance classes that are supported by a specific DB engine version in an AWS Region, run the following command.

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version \
--query "[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" \
--output text \
--region region
```

For Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version ^
--query "[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" ^
--output text ^
--region region
```

For example, the following command lists the supported DB instance classes for version 13.6 of the RDS for PostgreSQL DB engine in US East (N. Virginia).

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options --engine postgres --engine-version 13.6 \
--query "[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" \
--output text \
--region us-east-1
```

For Windows:

```
aws rds describe-orderable-db-instance-options --engine postgres --engine-version 13.6 ^
--query "[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" ^
--output text ^
--region us-east-1
```

Listing the DB engine versions that support a specific DB instance class in an AWS Region

To list the DB engine versions that support a specific DB instance class in an AWS Region, run the following command.

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class \
--query "[].{EngineVersion:EngineVersion,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" \
--output text \
--region region
```

For Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class ^
--query "[].{EngineVersion:EngineVersion,StorageType:StorageType}|[? \
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" ^
--output text ^
--region region
```

For example, the following command lists the DB engine versions of the RDS for PostgreSQL DB engine that support the db.r5.large DB instance class in US East (N. Virginia).

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options --engine postgres --db-instance-class db.r5.large \
    --query "[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?StorageType=='gp2']|[].{EngineVersion:EngineVersion}" \
    --output text \
    --region us-east-1
```

For Windows:

```
aws rds describe-orderable-db-instance-options --engine postgres --db-instance-class db.r5.large ^
    --query "[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?StorageType=='gp2']|[].{EngineVersion:EngineVersion}" ^
    --output text ^
    --region us-east-1
```

Changing your DB instance class

You can change the CPU and memory available to a DB instance by changing its DB instance class. To change the DB instance class, modify your DB instance by following the instructions in [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Configuring the processor for a DB instance class

Amazon RDS DB instance classes support Intel Hyper-Threading Technology, which enables multiple threads to run concurrently on a single Intel Xeon CPU core. Each thread is represented as a virtual CPU (vCPU) on the DB instance. A DB instance has a default number of CPU cores, which varies according to DB instance class. For example, a db.m4.xlarge DB instance class has two CPU cores and two threads per core by default—four vCPUs in total.

Note

Each vCPU is a hyperthread of an Intel Xeon CPU core.

Topics

- [Overview of configuring the processor \(p. 42\)](#)
- [DB instance classes that support processor configuration \(p. 43\)](#)
- [Setting the CPU cores and threads per CPU core for a DB instance class \(p. 47\)](#)

Overview of configuring the processor

In most cases, you can find a DB instance class that has a combination of memory and number of vCPUs to suit your workloads. However, you can also specify the following processor features to optimize your DB instance for specific workloads or business needs:

- **Number of CPU cores** – You can customize the number of CPU cores for the DB instance. You might do this to potentially optimize the licensing costs of your software with a DB instance that has sufficient amounts of RAM for memory-intensive workloads but fewer CPU cores.
- **Threads per core** – You can disable Intel Hyper-Threading Technology by specifying a single thread per CPU core. You might do this for certain workloads, such as high-performance computing (HPC) workloads.

You can control the number of CPU cores and threads for each core separately. You can set one or both in a request. After a setting is associated with a DB instance, the setting persists until you change it.

The processor settings for a DB instance are associated with snapshots of the DB instance. When a snapshot is restored, its restored DB instance uses the processor feature settings used when the snapshot was taken.

If you modify the DB instance class for a DB instance with nondefault processor settings, either specify default processor settings or explicitly specify processor settings at modification. This requirement ensures that you are aware of the third-party licensing costs that might be incurred when you modify the DB instance.

There is no additional or reduced charge for specifying processor features on an Amazon RDS DB instance. You're charged the same as for DB instances that are launched with default CPU configurations.

DB instance classes that support processor configuration

You can configure the number of CPU cores and threads per core only when the following conditions are met:

- You're configuring an Oracle DB instance. For information about the DB instance classes supported by different Oracle database editions, see [RDS for Oracle instance classes \(p. 1477\)](#).
- Your instance is using the Bring Your Own License (BYOL) licensing option. For more information about Oracle licensing options, see [RDS for Oracle licensing options \(p. 1474\)](#).
- Your instance doesn't belong to one of the db.r5 or db.r5b instance classes that have predefined processor configurations. These instance classes have names in the form db.r5.*instance_size*.tpc*threads_per_core*.mem*ratio* or db.r5b.*instance_size*.tpc*threads_per_core*.mem*ratio*. For example, db.r5b.xlarge.tpc2.mem4x is preconfigured with 2 threads per core (tpc2) and 4x as much memory as the standard db.r5b.xlarge instance class. You can't configure the processor features of these optimized instance classes. For more information, see [Supported RDS for Oracle instance classes \(p. 1477\)](#).

In the following table, you can find the DB instance classes that support setting a number of CPU cores and CPU threads per core. You can also find the default value and the valid values for the number of CPU cores and CPU threads per core for each DB instance class.

DB instance class	Default vCPUs	Default CPU cores	Default threads per core	Valid number of CPU cores	Valid number of threads per core
db.m5.large	2	1	2	1	1, 2
db.m5.xlarge	4	2	2	2	1, 2
db.m5.2xlarge	8	4	2	2, 4	1, 2
db.m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18,	1, 2

DB instance class	Default vCPUs	Default CPU cores	Default threads per core	Valid number of CPU cores	Valid number of threads per core
				20, 22, 24, 26, 28, 30, 32	
db.m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.m5d.large	2	1	2	1	1, 2
db.m5d.xlarge	4	2	2	2	1, 2
db.m5d.2xlarge	8	4	2	2, 4	1, 2
db.m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
db.m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5.large	2	1	2	1	1, 2
db.r5.xlarge	4	2	2	2	1, 2
db.r5.2xlarge	8	4	2	2, 4	1, 2
db.r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

DB instance class	Default vCPUs	Default CPU cores	Default threads per core	Valid number of CPU cores	Valid number of threads per core
db.r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r5b.large	2	1	2	1	1, 2
db.r5b.xlarge	4	2	2	2	1, 2
db.r5b.2xlarge	8	4	2	2, 4	1, 2
db.r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5b.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r5d.large	2	1	2	1	1, 2
db.r5d.xlarge	4	2	2	2	1, 2
db.r5d.2xlarge	8	4	2	2, 4	1, 2
db.r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

DB instance class	Default vCPUs	Default CPU cores	Default threads per core	Valid number of CPU cores	Valid number of threads per core
db.r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r4.large	2	1	2	1	1, 2
db.r4.xlarge	4	2	2	1, 2	1, 2
db.r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
db.r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r3.large	2	1	2	1	1, 2
db.r3.xlarge	4	2	2	1, 2	1, 2
db.r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2

DB instance class	Default vCPUs	Default CPU cores	Default threads per core	Valid number of CPU cores	Valid number of threads per core
db.x1e.xlarge	4	2	2	1, 2	1, 2
db.x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
db.x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
db.z1d.large	2	1	2	1	1, 2
db.z1d.xlarge	4	2	2	2	1, 2
db.z1d.2xlarge	8	4	2	2, 4	1, 2
db.z1d.3xlarge	12	6	2	2, 4, 6	1, 2
db.z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
db.z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Note

You can use AWS CloudTrail to monitor and audit changes to the process configuration of Amazon RDS for Oracle DB instances. For more information about using CloudTrail, see [Monitoring Amazon RDS API calls in AWS CloudTrail \(p. 725\)](#).

Setting the CPU cores and threads per CPU core for a DB instance class

You can configure the number of CPU cores and threads per core for the DB instance class when you perform the following operations:

- [Creating an Amazon RDS DB instance \(p. 230\)](#)
- [Modifying an Amazon RDS DB instance \(p. 327\)](#)
- [Restoring from a DB snapshot \(p. 452\)](#)
- [Restoring a DB instance to a specified time \(p. 499\)](#)
- [Restoring a backup into a MySQL DB instance \(p. 1361\)](#)

Note

When you modify a DB instance to configure the number of CPU cores or threads per core, there is a brief DB instance outage.

You can set the CPU cores and the threads per CPU core for a DB instance class using the AWS Management Console, the AWS CLI, or the RDS API.

Console

When you are creating, modifying, or restoring a DB instance, you set the DB instance class in the AWS Management Console. The **Instance specifications** section shows options for the processor. The following image shows the processor features options.

Instance specifications

Estimate your monthly costs for the DB Instance using the [AWS Simple Monthly Calculator](#)

DB engine
Oracle Database Enterprise Edition

License model [Info](#)
bring-your-own-license

DB engine version [Info](#)
Oracle 12.1.0.2.v12

DB instance class [Info](#)
db.r4.xlarge — 4 vCPU, 30.5 GiB RAM

Multi-AZ deployment [Info](#)
 Create replica in different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
 No

Storage type [Info](#)
Provisioned IOPS (SSD)

Allocated storage
100 GiB
(Minimum: 100 GiB, Maximum: 16384 GiB)

Provisioned IOPS [Info](#)
1000

▼ Additional configuration

Processor features

Override default values
You can change the number of CPU cores and threads per core on the DB instance class.

Core count [Info](#)
2

Threads per core [Info](#)
2

Set the following options to the appropriate values for your DB instance class under **Processor features**:

- **Core count** – Set the number of CPU cores using this option. The value must be equal to or less than the maximum number of CPU cores for the DB instance class.
- **Threads per core** – Specify **2** to enable multiple threads per core, or specify **1** to disable multiple threads per core.

When you modify or restore a DB instance, you can also set the CPU cores and the threads per CPU core to the defaults for the instance class.

When you view the details for a DB instance in the console, you can view the processor information for its DB instance class on the **Configuration** tab. The following image shows a DB instance class with one CPU core and multiple threads per core enabled.

Instance and IOPS	
Instance Class	db.r4.large
Core count	1
Threads per core	2
vCPU enabled	2
Storage Type	Provisioned IOPS (SSD)
IOPS	1000
Storage	100 GiB

For Oracle DB instances, the processor information only appears for Bring Your Own License (BYOL) DB instances.

AWS CLI

You can set the processor features for a DB instance when you run one of the following AWS CLI commands:

- [create-db-instance](#)

- [modify-db-instance](#)
- [restore-db-instance-from-db-snapshot](#)
- [restore-db-instance-from-s3](#)
- [restore-db-instance-to-point-in-time](#)

To configure the processor of a DB instance class for a DB instance by using the AWS CLI, include the `--processor-features` option in the command. Specify the number of CPU cores with the `coreCount` feature name, and specify whether multiple threads per core are enabled with the `threadsPerCore` feature name.

The option has the following syntax.

```
--processor-features "Name=coreCount,Value=<value>" "Name=threadsPerCore,Value=<value>"
```

The following are examples that configure the processor:

Examples

- [Setting the number of CPU cores for a DB instance \(p. 51\)](#)
- [Setting the number of CPU cores and disabling multiple threads for a DB instance \(p. 51\)](#)
- [Viewing the valid processor values for a DB instance class \(p. 52\)](#)
- [Returning to default processor settings for a DB instance \(p. 53\)](#)
- [Returning to the default number of CPU cores for a DB instance \(p. 53\)](#)
- [Returning to the default number of threads per core for a DB instance \(p. 54\)](#)

Setting the number of CPU cores for a DB instance

Example

The following example modifies `mydbinstance` by setting the number of CPU cores to 4. The changes are applied immediately by using `--apply-immediately`. If you want to apply the changes during the next scheduled maintenance window, omit the `--apply-immediately` option.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--processor-features "Name=coreCount,Value=4" \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--processor-features "Name=coreCount,Value=4" ^
--apply-immediately
```

Setting the number of CPU cores and disabling multiple threads for a DB instance

Example

The following example modifies `mydbinstance` by setting the number of CPU cores to 4 and disabling multiple threads per core. The changes are applied immediately by using `--apply-immediately`. If you want to apply the changes during the next scheduled maintenance window, omit the `--apply-immediately` option.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--processor-features "Name=coreCount,Value=4" "Name=threadsPerCore,Value=1" \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--processor-features "Name=coreCount,Value=4" "Name=threadsPerCore,Value=1" ^
--apply-immediately
```

Viewing the valid processor values for a DB instance class

Example

You can view the valid processor values for a particular DB instance class by running the [describe-orderable-db-instance-options](#) command and specifying the instance class for the --db-instance-class option. For example, the output for the following command shows the processor options for the db.r3.large instance class.

```
aws rds describe-orderable-db-instance-options --engine oracle-ee --db-instance-class db.r3.large
```

Following is sample output for the command in JSON format.

```
{
    "SupportsIops": true,
    "MaxIopsPerGib": 50.0,
    "LicenseModel": "bring-your-own-license",
    "DBInstanceClass": "db.r3.large",
    "SupportsIAMDatabaseAuthentication": false,
    "MinStorageSize": 100,
    "AvailabilityZones": [
        {
            "Name": "us-west-2a"
        },
        {
            "Name": "us-west-2b"
        },
        {
            "Name": "us-west-2c"
        }
    ],
    "EngineVersion": "12.1.0.2.v2",
    "MaxStorageSize": 32768,
    "MinIopsPerGib": 1.0,
    "MaxIopsPerDbInstance": 40000,
    "ReadReplicaCapable": false,
    "AvailableProcessorFeatures": [
        {
            "Name": "coreCount",
            "DefaultValue": "1",
            "AllowedValues": "1"
        },
        {
            "Name": "threadsPerCore",
            "DefaultValue": "2",
            "AllowedValues": "1,2"
        }
    ]
},
```

```
        "SupportsEnhancedMonitoring": true,  
        "SupportsPerformanceInsights": false,  
        "MinIopsPerDbInstance": 1000,  
        "StorageType": "io1",  
        "Vpc": false,  
        "SupportsStorageEncryption": true,  
        "Engine": "oracle-ee",  
        "MultiAZCapable": true  
    }
```

In addition, you can run the following commands for DB instance class processor information:

- [describe-db-instances](#) – Shows the processor information for the specified DB instance.
- [describe-db-snapshots](#) – Shows the processor information for the specified DB snapshot.
- [describe-valid-db-instance-modifications](#) – Shows the valid modifications to the processor for the specified DB instance.

In the output of the preceding commands, the values for the processor features are not null only if the following conditions are met:

- You are using an Oracle DB instance.
- Your Oracle DB instance supports changing processor values.
- The current CPU core and thread settings are set to nondefault values.

If the preceding conditions aren't met, you can get the instance type using [describe-db-instances](#). You can get the processor information for this instance type by running the EC2 operation [describe-instance-types](#).

Returning to default processor settings for a DB instance

Example

The following example modifies mydbinstance by returning its DB instance class to the default processor values for it. The changes are applied immediately by using `--apply-immediately`. If you want to apply the changes during the next scheduled maintenance window, omit the `--apply-immediately` option.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
  --use-default-processor-features \  
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^  
  --use-default-processor-features ^  
  --apply-immediately
```

Returning to the default number of CPU cores for a DB instance

Example

The following example modifies mydbinstance by returning its DB instance class to the default number of CPU cores for it. The threads per core setting isn't changed. The changes are applied immediately by using `--apply-immediately`. If you want to apply the changes during the next scheduled maintenance window, omit the `--apply-immediately` option.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--processor-features "Name=coreCount,Value=DEFAULT" \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--processor-features "Name=coreCount,Value=DEFAULT" ^
--apply-immediately
```

Returning to the default number of threads per core for a DB instance

Example

The following example modifies mydbinstance by returning its DB instance class to the default number of threads per core for it. The number of CPU cores setting isn't changed. The changes are applied immediately by using --apply-immediately. If you want to apply the changes during the next scheduled maintenance window, omit the --apply-immediately option.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--processor-features "Name=threadsPerCore,Value=DEFAULT" \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--processor-features "Name=threadsPerCore,Value=DEFAULT" ^
--apply-immediately
```

RDS API

You can set the processor features for a DB instance when you call one of the following Amazon RDS API operations:

- [CreateDBInstance](#)
- [ModifyDBInstance](#)
- [RestoreDBInstanceFromDBSnapshot](#)
- [RestoreDBInstanceFromS3](#)
- [RestoreDBInstanceToPointInTime](#)

To configure the processor features of a DB instance class for a DB instance by using the Amazon RDS API, include the `ProcessFeatures` parameter in the call.

The parameter has the following syntax.

```
ProcessFeatures "Name=coreCount,Value=<value>" "Name=threadsPerCore,Value=<value>"
```

Specify the number of CPU cores with the `coreCount` feature name, and specify whether multiple threads per core are enabled with the `threadsPerCore` feature name.

You can view the valid processor values for a particular instance class by running the [DescribeOrderableDBInstanceState](#) operation and specifying the instance class for the `DBInstanceState` parameter. You can also use the following operations:

- [DescribeDBInstances](#) – Shows the processor information for the specified DB instance.
- [DescribeDBSnapshots](#) – Shows the processor information for the specified DB snapshot.
- [DescribeValidDBInstanceModifications](#) – Shows the valid modifications to the processor for the specified DB instance.

In the output of the preceding operations, the values for the processor features are not null only if the following conditions are met:

- You are using an Oracle DB instance.
- Your Oracle DB instance supports changing processor values.
- The current CPU core and thread settings are set to nondefault values.

If the preceding conditions aren't met, you can get the instance type using [DescribeDBInstances](#). You can get the processor information for this instance type by running the EC2 operation [DescribeInstanceTypes](#).

Hardware specifications for DB instance classes

The following terminology is used to describe hardware specifications for DB instance classes:

vCPU

The number of virtual central processing units (CPUs). A *virtual CPU* is a unit of capacity that you can use to compare DB instance classes. Instead of purchasing or leasing a particular processor to use for several months or years, you are renting capacity by the hour. Our goal is to make a consistent and specific amount of CPU capacity available, within the limits of the actual underlying hardware.

ECU

The relative measure of the integer processing power of an Amazon EC2 instance. To make it easy for developers to compare CPU capacity between different instance classes, we have defined an Amazon EC2 Compute Unit. The amount of CPU that is allocated to a particular instance is expressed in terms of these EC2 Compute Units. One ECU currently provides CPU capacity equivalent to a 1.0–1.2 GHz 2007 Opteron or 2007 Xeon processor.

Memory (GiB)

The RAM, in gibibytes, allocated to the DB instance. There is often a consistent ratio between memory and vCPU. As an example, take the db.r4 instance class, which has a memory to vCPU ratio similar to the db.r5 instance class. However, for most use cases the db.r5 instance class provides better, more consistent performance than the db.r4 instance class.

EBS-Optimized

The DB instance uses an optimized configuration stack and provides additional, dedicated capacity for I/O. This optimization provides the best performance by minimizing contention between I/O and other traffic from your instance. For more information about Amazon EBS-optimized instances, see [Amazon EBS-Optimized instances](#) in the *Amazon EC2 User Guide for Linux Instances*.

Max. Bandwidth (Mbps)

The maximum bandwidth in megabits per second. Divide by 8 to get the expected throughput in megabytes per second.

Important

General Purpose SSD (gp2) volumes for Amazon RDS DB instances have a throughput limit of 250 MiB/s in most cases. However, the throughput limit can vary depending on volume size. For more information, see [Amazon EBS volume types](#) in the *Amazon EC2 User Guide for Linux Instances*.

Network Performance

The network speed relative to other DB instance classes.

In the following table, you can find hardware details about the Amazon RDS DB instance classes.

For information about Amazon RDS DB engine support for each DB instance class, see [Supported DB engines for DB instance classes \(p. 12\)](#).

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.m6g – general-purpose instance classes powered by AWS Graviton2 processors							
db.m6g.16xlarge	64	—	256	Yes	19,000	25 Gbps	
db.m6g.12xlarge	48	—	192	Yes	13,500	20 Gbps	
db.m6g.8xlarge	32	—	128	Yes	9,500	12 Gbps	
db.m6g.4xlarge	16	—	64	Yes	6,800	Up to 10 Gbps	
db.m6g.2xlarge*	8	—	32	Yes	Up to 4,750	Up to 10 Gbps	
db.m6g.xlarge*	4	—	16	Yes	Up to 4,750	Up to 10 Gbps	
db.m6g.large*	2	—	8	Yes	Up to 4,750	Up to 10 Gbps	
db.m6gd							
db.m6gd.16xlarge	64	—	256	Yes	19,000	25 Gbps	
db.m6gd.12xlarge	48	—	192	Yes	13,500	20 Gbps	
db.m6gd.8xlarge	32	—	128	Yes	9,000	12 Gbps	
db.m6gd.4xlarge	16	—	64	Yes	4,750	Up to 10 Gbps	
db.m6gd.2xlarge	8	—	32	Yes	Up to 4,750	Up to 10 Gbps	
db.m6gd.xlarge	4	—	16	Yes	Up to 4,750	Up to 10 Gbps	
db.m6gd.large	2	—	8	Yes	Up to 4,750	Up to 10 Gbps	
db.m6i – general-purpose instance classes							
db.m6i.32xlarge	128	—	512	Yes	50,000	40 Gbps	
db.m6i.24xlarge	96	—	384	Yes	37,500	30 Gbps	
db.m6i.16xlarge	64	—	256	Yes	25,000	20 Gbps	

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.m6i.12xlarge	48	—	192	Yes	18,750	15 Gbps	
db.m6i.8xlarge	32	—	128	Yes	12,500	10 Gbps	
db.m6i.4xlarge*	16	—	64	Yes	Up to 12,500	Up to 10 Gbps	
db.m6i.2xlarge*	8	—	32	Yes	Up to 12,500	Up to 10 Gbps	
db.m6i.xlarge*	4	—	16	Yes	Up to 12,500	Up to 10 Gbps	
db.m6i.large*	2	—	8	Yes	Up to 12,500	Up to 10 Gbps	
db.m5d – general-purpose instance classes							
db.m5d.24xlarge	96	345	384	Yes	19,000	25 Gbps	
db.m5d.16xlarge	64	262	256	Yes	13,600	20 Gbps	
db.m5d.12xlarge	48	173	192	Yes	9,500	10 Gbps	
db.m5d.8xlarge	32	131	128	Yes	6,800	10 Gbps	
db.m5d.4xlarge	16	61	64	Yes	4,750	Up to 10 Gbps	
db.m5d.2xlarge*	8	31	32	Yes	Up to 4,750	Up to 10 Gbps	
db.m5d.xlarge*	4	15	16	Yes	Up to 4,750	Up to 10 Gbps	
db.m5d.large*	2	10	8	Yes	Up to 4,750	Up to 10 Gbps	
db.m5 – general-purpose instance classes							
db.m5.24xlarge	96	345	384	Yes	19,000	25 Gbps	
db.m5.16xlarge	64	262	256	Yes	13,600	20 Gbps	
db.m5.12xlarge	48	173	192	Yes	9,500	10 Gbps	
db.m5.8xlarge	32	131	128	Yes	6,800	10 Gbps	
db.m5.4xlarge	16	61	64	Yes	4,750	Up to 10 Gbps	
db.m5.2xlarge*	8	31	32	Yes	Up to 4,750	Up to 10 Gbps	
db.m5.xlarge*	4	15	16	Yes	Up to 4,750	Up to 10 Gbps	

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.m5.large*	2	10	8	Yes	Up to 4,750	Up to 10 Gbps	
db.m4 – general-purpose instance classes							
db.m4.16xlarge	64	188	256	Yes	10,000	25 Gbps	
db.m4.10xlarge	40	124.5	160	Yes	4,000	10 Gbps	
db.m4.4xlarge	16	53.5	64	Yes	2,000	High	
db.m4.2xlarge	8	25.5	32	Yes	1,000	High	
db.m4.xlarge	4	13	16	Yes	750	High	
db.m4.large	2	6.5	8	Yes	450	Moderate	
db.m3 – general-purpose instance classes							
db.m3.2xlarge	8	26	30	Yes	1,000	High	
db.m3.xlarge	4	13	15	Yes	500	High	
db.m3.large	2	6.5	7.5	No	—	Moderate	
db.m3.medium	1	3	3.75	No	—	Moderate	
db.m1 – general-purpose instance classes							
db.m1.xlarge	4	4	15	Yes	450	High	
db.m1.large	2	2	7.5	Yes	450	Moderate	
db.m1.medium	1	1	3.75	No	—	Moderate	
db.m1.small	1	1	1.7	No	—	Very Low	
db.x2g – memory-optimized instance classes							
db.x2g.16xlarge	64	—	1024	Yes	19,000	25 Gbps	
db.x2g.12xlarge	48	—	768	Yes	14,250	20 Gbps	
db.x2g.8xlarge	32	—	512	Yes	9,500	12 Gbps	
db.x2g.4xlarge	16	—	256	Yes	4,750	Up to 10 Gbps	
db.x2g.2xlarge	8	—	128	Yes	Up to 4,750	Up to 10 Gbps	
db.x2g.xlarge	4	—	64	Yes	Up to 4,750	Up to 10 Gbps	
db.x2g.large	2	—	32	Yes	Up to 4,750	Up to 10 Gbps	
db.z1d – memory-optimized instance classes							

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.z1d.12xlarge	48	271	384	Yes	14,000	25 Gbps	
db.z1d.6xlarge	24	134	192	Yes	7,000	10 Gbps	
db.z1d.3xlarge	12	75	96	Yes	3,500	Up to 10 Gbps	
db.z1d.2xlarge	8	53	64	Yes	2,333	Up to 10 Gbps	
db.z1d.xlarge*	4	28	32	Yes	Up to 2,333	Up to 10 Gbps	
db.z1d.large*	2	15	16	Yes	Up to 2,333	Up to 10 Gbps	
db.x1e – memory-optimized instance classes							
db.x1e.32xlarge	128	340	3,904	Yes	14,000	25 Gbps	
db.x1e.16xlarge	64	179	1,952	Yes	7,000	10 Gbps	
db.x1e.8xlarge	32	91	976	Yes	3,500	Up to 10 Gbps	
db.x1e.4xlarge	16	47	488	Yes	1,750	Up to 10 Gbps	
db.x1e.2xlarge	8	23	244	Yes	1,000	Up to 10 Gbps	
db.x1e.xlarge	4	12	122	Yes	500	Up to 10 Gbps	
db.x1 – memory-optimized instance classes							
db.x1.32xlarge	128	349	1,952	Yes	14,000	25 Gbps	
db.x1.16xlarge	64	174.5	976	Yes	7,000	10 Gbps	
db.r6g – memory-optimized instance classes powered by AWS Graviton2 processors							
db.r6g.16xlarge	64	—	512	Yes	19,000	25 Gbps	
db.r6g.12xlarge	48	—	384	Yes	13,500	20 Gbps	
db.r6g.8xlarge	32	—	256	Yes	9,000	12 Gbps	
db.r6g.4xlarge	16	—	128	Yes	4,750	Up to 10 Gbps	
db.r6g.2xlarge*	8	—	64	Yes	Up to 4,750	Up to 10 Gbps	
db.r6g.xlarge*	4	—	32	Yes	Up to 4,750	Up to 10 Gbps	

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.r6g.large*	2	—	16	Yes	Up to 4,750	Up to 10 Gbps	
db.r6gd							
db.r6gd.16xlarge	64	—	512	Yes	19,000	25 Gbps	
db.r6gd.12xlarge	48	—	384	Yes	13,500	20 Gbps	
db.r6gd.8xlarge	32	—	256	Yes	9,000	12 Gbps	
db.r6gd.4xlarge	16	—	128	Yes	4,750	Up to 10 Gbps	
db.r6gd.2xlarge	8	—	64	Yes	Up to 4,750	Up to 10 Gbps	
db.r6gd.xlarge	4	—	32	Yes	Up to 4,750	Up to 10 Gbps	
db.r6gd.large	2	—	16	Yes	Up to 4,750	Up to 10 Gbps	
db.r6i – memory-optimized instance classes							
db.r6i.32xlarge	128	—	1,024	Yes	Yes	40,000	50 Gbps
db.r6i.24xlarge	96	—	768	Yes	Yes	30,000	37.5 Gbps
db.r6i.16xlarge	64	—	512	Yes	Yes	20,000	25 Gbps
db.r6i.12xlarge	48	—	384	Yes	Yes	15,000	18.75 Gbps
db.r6i.8xlarge	32	—	256	Yes	Yes	10,000	12.5 Gbps
db.r6i.4xlarge*	16	—	128	Yes	Yes	Up to 10,000	Up to 12.5 Gbps
db.r6i.2xlarge*	8	—	64	Yes	Yes	Up to 10,000	Up to 12.5 Gbps
db.r6i.xlarge*	4	—	32	Yes	Yes	Up to 10,000	Up to 12.5 Gbps
db.r6i.large*	2	—	16	Yes	Yes	Up to 10,000	Up to 12.5 Gbps
db.r5d – memory-optimized instance classes							
db.r5d.24xlarge	96	347	768	Yes	19,000	25 Gbps	
db.r5d.16xlarge	64	264	512	Yes	13,600	20 Gbps	
db.r5d.12xlarge	48	173	384	Yes	9,500	10 Gbps	
db.r5d.8xlarge	32	132	256	Yes	6,800	10 Gbps	

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.r5d.4xlarge	16	71	128	Yes	4,750	Up to 10 Gbps	
db.r5d.2xlarge*	8	38	64	Yes	Up to 4,750	Up to 10 Gbps	
db.r5d.xlarge*	4	19	32	Yes	Up to 4,750	Up to 10 Gbps	
db.r5d.large*	2	10	16	Yes	Up to 4,750	Up to 10 Gbps	
db.r5b – memory-optimized instance classes							
db.r5b.24xlarge	96	347	768	Yes	60,000	25 Gbps	
db.r5b.16xlarge	64	264	512	Yes	40,000	20 Gbps	
db.r5b.12xlarge	48	173	384	Yes	30,000	10 Gbps	
db.r5b.8xlarge	32	132	256	Yes	20,000	10 Gbps	
db.r5b.4xlarge	16	71	128	Yes	10,000	Up to 10 Gbps	
db.r5b.2xlarge*	8	38	64	Yes	Up to 10,000	Up to 10 Gbps	
db.r5b.xlarge*	4	19	32	Yes	Up to 10,000	Up to 10 Gbps	
db.r5b.large*	2	10	16	Yes	Up to 10,000	Up to 10 Gbps	
db.r5 – memory-optimized instance classes							
db.r5.24xlarge	96	347	768	Yes	19,000	25 Gbps	
db.r5.16xlarge	64	264	512	Yes	13,600	20 Gbps	
db.r5.12xlarge	48	173	384	Yes	9,500	10 Gbps	
db.r5.8xlarge	32	132	256	Yes	6,800	10 Gbps	
db.r5.4xlarge	16	71	128	Yes	4,750	Up to 10 Gbps	
db.r5.2xlarge*	8	38	64	Yes	Up to 4,750	Up to 10 Gbps	
db.r5.xlarge*	4	19	32	Yes	Up to 4,750	Up to 10 Gbps	
db.r5.large*	2	10	16	Yes	Up to 4,750	Up to 10 Gbps	
db.r4 – memory-optimized instance classes							

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.r4.16xlarge	64	195	488	Yes	14,000	25 Gbps	
db.r4.8xlarge	32	99	244	Yes	7,000	10 Gbps	
db.r4.4xlarge	16	53	122	Yes	3,500	Up to 10 Gbps	
db.r4.2xlarge	8	27	61	Yes	1,700	Up to 10 Gbps	
db.r4.xlarge	4	13.5	30.5	Yes	850	Up to 10 Gbps	
db.r4.large	2	7	15.25	Yes	425	Up to 10 Gbps	
db.r3 – memory-optimized instance classes							
db.r3.8xlarge	32	104	244	No	—	10 Gbps	
db.r3.4xlarge	16	52	122	Yes	2,000	High	
db.r3.2xlarge	8	26	61	Yes	1,000	High	
db.r3.xlarge	4	13	30.5	Yes	500	Moderate	
db.r3.large	2	6.5	15.25	No	—	Moderate	
db.t4g – burstable-performance instance classes							
db.t4g.2xlarge*	8	—	32	Yes	Up to 2,780	Up to 5 Gbps	
db.t4g.xlarge*	4	—	16	Yes	Up to 2,780	Up to 5 Gbps	
db.t4g.large*	2	—	8	Yes	Up to 2,780	Up to 5 Gbps	
db.t4g.medium*	2	—	4	Yes	Up to 2,085	Up to 5 Gbps	
db.t4g.small*	2	—	2	Yes	Up to 2,085	Up to 5 Gbps	
db.t4g.micro*	2	—	1	Yes	Up to 2,085	Up to 5 Gbps	
db.t3 – burstable-performance instance classes							
db.t3.2xlarge*	8	Variable	32	Yes	Up to 2,048	Up to 5 Gbps	
db.t3.xlarge*	4	Variable	16	Yes	Up to 2,048	Up to 5 Gbps	

Instance class	vCPU	ECU	Memory (GiB)	EBS optimized	Max. bandwidth (mbps)	Network performance	
db.t3.large*	2	Variable	8	Yes	Up to 2,048	Up to 5 Gbps	
db.t3.medium*	2	Variable	4	Yes	Up to 1,536	Up to 5 Gbps	
db.t3.small*	2	Variable	2	Yes	Up to 1,536	Up to 5 Gbps	
db.t3.micro*	2	Variable	1	Yes	Up to 1,536	Up to 5 Gbps	

db.t2 – burstable-performance instance classes

db.t2.2xlarge	8	Variable	32	No	—	Moderate	
db.t2.xlarge	4	Variable	16	No	—	Moderate	
db.t2.large	2	Variable	8	No	—	Moderate	
db.t2.medium	2	Variable	4	No	—	Moderate	
db.t2.small	1	Variable	2	No	—	Low	
db.t2.micro	1	Variable	1	No	—	Low	

* These DB instance classes can support maximum performance for 30 minutes at least once every 24 hours. For more information on baseline performance of these instance types, see [Amazon EBS-optimized instances](#) in the *Amazon EC2 User Guide for Linux Instances*.

** The r3.8xlarge instance doesn't have dedicated EBS bandwidth and therefore doesn't offer EBS optimization. On this instance, network traffic and Amazon EBS traffic share the same 10-gigabit network interface.

Amazon RDS DB instance storage

DB instances for Amazon RDS for MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server use Amazon Elastic Block Store (Amazon EBS) volumes for database and log storage. Depending on the amount of storage requested, Amazon RDS automatically stripes across multiple Amazon EBS volumes to enhance performance.

For more information about instance storage pricing, see [Amazon RDS pricing](#).

Amazon RDS storage types

Amazon RDS provides three storage types: General Purpose SSD (also known as gp2 and gp3), Provisioned IOPS SSD (also known as io1), and magnetic (also known as standard). They differ in performance characteristics and price, which means that you can tailor your storage performance and cost to the needs of your database workload. You can create MySQL, MariaDB, Oracle, and PostgreSQL RDS DB instances with up to 64 tebibytes (TiB) of storage. You can create SQL Server RDS DB instances with up to 16 TiB of storage. For this amount of storage, use the Provisioned IOPS SSD and General Purpose SSD storage types.

The following list briefly describes the three storage types:

- **General Purpose SSD** – General Purpose SSD volumes offer cost-effective storage that is ideal for a broad range of workloads running on medium-sized DB instances. General Purpose storage is best suited for development and testing environments.

For more information about General Purpose SSD storage, including the storage size ranges, see [General Purpose SSD storage \(p. 64\)](#).

- **Provisioned IOPS SSD** – Provisioned IOPS storage is designed to meet the needs of I/O-intensive workloads, particularly database workloads, that require low I/O latency and consistent I/O throughput. Provisioned IOPS storage is best suited for production environments.

For more information about Provisioned IOPS storage, including the storage size ranges, see [Provisioned IOPS SSD storage \(p. 66\)](#).

- **Magnetic** – Amazon RDS also supports magnetic storage for backward compatibility. We recommend that you use General Purpose SSD or Provisioned IOPS SSD for any new storage needs. The maximum amount of storage allowed for DB instances on magnetic storage is less than that of the other storage types. For more information, see [Magnetic storage \(p. 68\)](#).

General Purpose SSD storage

General Purpose SSD storage offers cost-effective storage that is acceptable for most database workloads that aren't latency sensitive. The following are the storage size ranges for General Purpose SSD DB instances:

- MariaDB, MySQL, Oracle, and PostgreSQL database instances: 20 GiB–64 TiB
- SQL Server Enterprise, Standard, Web, and Express Editions: 20 GiB–16 TiB

Note

DB instances that use General Purpose SSD storage can experience much longer latency after read replica creation, Multi-AZ conversion, and DB snapshot restoration than instances that use Provisioned IOPS storage. If you need a DB instance with minimum latency after these operations, we recommend using [Provisioned IOPS SSD storage \(p. 66\)](#).

Amazon RDS offers two types of General Purpose SSD storage: [gp2 storage \(p. 65\)](#) and [gp3 storage \(p. 65\)](#).

gp2 storage

When your applications don't need high storage performance, you can use General Purpose SSD gp2 storage. Baseline I/O performance for gp2 storage is 3 IOPS for each GiB, with a minimum of 100 IOPS. This relationship means that larger volumes have better performance. For example, baseline performance for a 100-GiB volume is 300 IOPS. Baseline performance for a 1-TiB volume is 3,000 IOPS. Maximum baseline performance for a gp2 volume (5.34 TiB and greater) is 16,000 IOPS.

Volumes below 1 TiB in size also have the ability to burst to 3,000 IOPS for extended periods of time. Instance I/O credit balance determines burst performance. For more information about instance I/O credits, see [I/O credits and burst performance](#) in the *Amazon EC2 User Guide*. For a more detailed description of how baseline performance and I/O credit balance affect performance, see the post [Understanding burst vs. baseline performance with Amazon RDS and gp2](#) on the AWS Database Blog.

Many workloads never deplete the burst balance. However, some workloads can exhaust the 3,000 IOPS burst storage credit balance, so you should plan your storage capacity to meet the needs of your workloads.

For gp2 volumes larger than 1 TiB, the baseline performance is greater than the burst performance. For such volumes, burst is often irrelevant because the baseline performance is better than the 3,000 IOPS burst performance. However, for DB instances larger than 1 TiB where the storage is *striped* across four Amazon EBS volumes, burst performance of up to 12,000 IOPS can be seen. This applies to RDS database engines other than Microsoft SQL Server, which doesn't support volume striping.

gp3 storage

By using General Purpose SSD gp3 storage volumes, you can customize storage performance independently of storage capacity. *Storage performance* is the combination of I/O operations per second (IOPS) and how fast the storage volume can perform reads and writes (storage throughput). On gp3 storage volumes, Amazon RDS provides a baseline storage performance of 3000 IOPS and 125 MiBps.

For every RDS DB engine except RDS for SQL Server, when the storage size for gp3 volumes reaches a certain threshold, the baseline storage performance increases to 12,000 IOPS and 500 MiBps. This is because of *volume striping*, where the storage uses four logical volumes instead of one. RDS for SQL Server doesn't support volume striping, and therefore doesn't have a threshold value.

Note

General Purpose SSD gp3 storage is supported on Single-AZ and Multi-AZ DB instances, but isn't supported on Multi-AZ DB clusters. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#) and [Multi-AZ DB cluster deployments \(p. 127\)](#).

Storage performance for gp3 volumes on Amazon RDS DB engines, including the threshold, is shown in the following table.

DB engine	Storage size	Baseline storage performance	Range of Provisioned IOPS	Range of provisioned storage throughput
MariaDB, MySQL, and PostgreSQL	Less than 400 GiB	3,000 IOPS/125 MiBps	N/A	N/A
MariaDB, MySQL, and PostgreSQL	400 GiB and higher	12,000 IOPS/500 MiBps	12,000–64,000 IOPS	500–4,000 MiBps
Oracle	Less than 200 GiB	3,000 IOPS/125 MiBps	N/A	N/A

DB engine	Storage size	Baseline storage performance	Range of Provisioned IOPS	Range of provisioned storage throughput
Oracle	200 GiB and higher	12,000 IOPS/500 MiBps	12,000–64,000 IOPS	500–4,000 MiBps
SQL Server	20 GiB–16 TiB	3,000 IOPS/125 MiBps	3,000–16,000 IOPS	125–1,000 MiBps

For every DB engine except RDS for SQL Server, you can provision additional IOPS and storage throughput when storage size is at or above the threshold value. For RDS for SQL Server, you can provision additional IOPS and storage throughput for any available storage size. For all DB engines, you pay for only the additional provisioned storage performance. For more information, see [Amazon RDS pricing](#).

Although the added Provisioned IOPS and storage throughput aren't dependent on the storage size, they are related to each other. When you raise the IOPS above 32,000 for MariaDB and MySQL, the storage throughput value automatically increases from 500 MiBps. For example, when you set the IOPS to 40,000 on RDS for MySQL, the storage throughput must be at least 625 MiBps. The automatic increase doesn't happen for Oracle, PostgreSQL, and SQL Server DB instances.

Storage performance values for gp3 volumes on RDS have the following constraints:

- The maximum ratio of storage throughput to IOPS is 0.25 for all supported DB engines.
- The minimum ratio of IOPS to allocated storage (in GiB) is 0.5 on RDS for SQL Server. There is no minimum ratio for the other supported DB engines.
- The maximum ratio of IOPS to allocated storage is 500 for all supported DB engines.
- If you're using storage autoscaling, the same ratios between IOPS and maximum storage threshold (in GiB) also apply.

For more information on storage autoscaling, see [Managing capacity automatically with Amazon RDS storage autoscaling \(p. 412\)](#).

Provisioned IOPS SSD storage

For a production application that requires fast and consistent I/O performance, we recommend Provisioned IOPS (I/O operations per second) storage. Provisioned IOPS storage is a storage type that delivers predictable performance, and consistently low latency. Provisioned IOPS storage is optimized for online transaction processing (OLTP) workloads that have consistent performance requirements. Provisioned IOPS helps performance tuning of these workloads.

In some cases, your database workload might not be able to achieve 100 percent of the IOPS that you have provisioned. For more information, see [Factors that affect storage performance \(p. 69\)](#).

When you create a DB instance, you specify the IOPS rate and the size of the volume. Amazon RDS provides that IOPS rate for the DB instance until you change it.

io1 storage

For I/O-intensive workloads, you can use Provisioned IOPS SSD io1 storage and achieve up to 256,000 I/O operations per second (IOPS). The following table shows the range of Provisioned IOPS and storage size for each database engine.

Database engine	Range of Provisioned IOPS	Range of storage size
MariaDB	1,000–256,000 IOPS	100 GiB–64 TiB
SQL Server	1,000–64,000 IOPS	20 GiB–16 TiB
MySQL	1,000–256,000 IOPS	100 GiB–64 TiB
Oracle	1,000–256,000 IOPS	100 GiB–64 TiB
PostgreSQL	1,000–256,000 IOPS	100 GiB–64 TiB

Note

For SQL Server, the maximum 64,000 IOPS is guaranteed only on [Nitro-based instances](#) that are on the m5*, m6i, r5*, r6i, and z1d instance types. Other instance types guarantee performance up to 32,000 IOPS.

For Oracle, you can provision the maximum 256,000 IOPS only on the r5b instance type.

The IOPS and storage size ranges have the following constraints:

- The ratio of IOPS to allocated storage (in GiB) must be from 1–50 on RDS for SQL Server, and 0.5–50 on other RDS DB engines.
- If you're using storage autoscaling, the same ratios between IOPS and maximum storage threshold (in GiB) also apply.

For more information on storage autoscaling, see [Managing capacity automatically with Amazon RDS storage autoscaling \(p. 412\)](#).

Combining Provisioned IOPS storage with Multi-AZ deployments or read replicas

For production OLTP use cases, we recommend that you use Multi-AZ deployments for enhanced fault tolerance with Provisioned IOPS storage for fast and predictable performance.

You can also use Provisioned IOPS SSD storage with read replicas for MySQL, MariaDB or PostgreSQL. The type of storage for a read replica is independent of that on the primary DB instance. For example, you might use General Purpose SSD for read replicas with a primary DB instance that uses Provisioned IOPS SSD storage to reduce costs. However, your read replica's performance in this case might differ from that of a configuration where both the primary DB instance and the read replicas use Provisioned IOPS SSD storage.

Provisioned IOPS storage costs

With Provisioned IOPS storage, you are charged for the provisioned resources whether or not you use them in a given month.

For more information about pricing, see [Amazon RDS pricing](#).

Getting the best performance from Amazon RDS Provisioned IOPS SSD storage

If your workload is I/O constrained, using Provisioned IOPS SSD storage can increase the number of I/O requests that the system can process concurrently. Increased concurrency allows for decreased latency

because I/O requests spend less time in a queue. Decreased latency allows for faster database commits, which improves response time and allows for higher database throughput.

Provisioned IOPS SSD storage provides a way to reserve I/O capacity by specifying IOPS. However, as with any other system capacity attribute, its maximum throughput under load is constrained by the resource that is consumed first. That resource might be network bandwidth, CPU, memory, or database internal resources.

For more information about getting the most out of your Provisioned IOPS volumes, see [Amazon EBS volume performance](#).

Comparing solid-state drive (SSD) storage types

The following table shows use cases and performance characteristics for the SSD storage volumes used by Amazon RDS.

Characteristic	Provisioned IOPS (io1)	General Purpose (gp3)	General Purpose (gp2)
Description	Consistent storage performance (IOPS, throughput, latency) Designed for latency-sensitive, transactional workloads.	Flexibility in provisioning storage, IOPS, and throughput independently Balances price performance for a wide variety of transactional workloads	Provides burstable IOPS Balances price performance for a wide variety of transactional workloads
Use cases	Transactional workloads that require sustained IOPS performance up to 256,000 IOPS	Broad range of workloads running on medium-sized relational databases in development/test environments	Broad range of workloads running on medium-sized relational databases in development/test environments
Latency	Single-digit millisecond, provided consistently 99.9% of the time	Single-digit millisecond, provided consistently 99% of the time	Single-digit millisecond, provided consistently 99% of the time
Volume size	100 GiB–64 TiB (16 TiB on RDS for SQL Server)	20 GiB–64 TiB (16 TiB on RDS for SQL Server)	20 GiB–64 TiB (16 TiB on RDS for SQL Server)
Maximum IOPS	256,000 (64,000 on RDS for SQL Server)	64,000 (16,000 on RDS for SQL Server)	16,000
Maximum throughput	Scales based on Provisioned IOPS up to 4,000 MB/s	Provision additional throughput up to 4,000 MB/s	250 MB/s
AWS CLI and RDS API name	io1	gp3	gp2

Magnetic storage

Amazon RDS also supports magnetic storage for backward compatibility. We recommend that you use General Purpose SSD or Provisioned IOPS SSD for any new storage needs. The following are some limitations for magnetic storage:

- Doesn't allow you to scale storage when using the SQL Server database engine.
- Doesn't support storage autoscaling.
- Doesn't support elastic volumes.
- Limited to a maximum size of 3 TiB.
- Limited to a maximum of 1,000 IOPS.

Monitoring storage performance

Amazon RDS provides several metrics that you can use to determine how your DB instance is performing. You can view the metrics on the summary page for your instance in Amazon RDS Management Console. You can also use Amazon CloudWatch to monitor these metrics. For more information, see [Viewing metrics in the Amazon RDS console \(p. 525\)](#). Enhanced Monitoring provides more detailed I/O metrics; for more information, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

The following metrics are useful for monitoring storage for your DB instance:

- **IOPS** – The number of I/O operations completed each second. This metric is reported as the average IOPS for a given time interval. Amazon RDS reports read and write IOPS separately on 1-minute intervals. Total IOPS is the sum of the read and write IOPS. Typical values for IOPS range from zero to tens of thousands per second.
- **Latency** – The elapsed time between the submission of an I/O request and its completion. This metric is reported as the average latency for a given time interval. Amazon RDS reports read and write latency separately at 1-minute intervals. Typical values for latency are in milliseconds (ms).
- **Throughput** – The number of bytes each second that are transferred to or from disk. This metric is reported as the average throughput for a given time interval. Amazon RDS reports read and write throughput separately on 1-minute intervals using units of megabytes per second (MB/s). Typical values for throughput range from zero to the I/O channel's maximum bandwidth.
- **Queue Depth** – The number of I/O requests in the queue waiting to be serviced. These are I/O requests that have been submitted by the application but have not been sent to the device because the device is busy servicing other I/O requests. Time spent waiting in the queue is a component of latency and service time (not available as a metric). This metric is reported as the average queue depth for a given time interval. Amazon RDS reports queue depth in 1-minute intervals. Typical values for queue depth range from zero to several hundred.

Measured IOPS values are independent of the size of the individual I/O operation. This means that when you measure I/O performance, make sure to look at the throughput of the instance, not simply the number of I/O operations.

Factors that affect storage performance

System activities, database workload, and DB instance class can affect storage performance.

System activities

The following system-related activities consume I/O capacity and might reduce DB instance performance while in progress:

- Multi-AZ standby creation
- Read replica creation
- Changing storage types

Database workload

In some cases, your database or application design results in concurrency issues, locking, or other forms of database contention. In these cases, you might not be able to use all the provisioned bandwidth directly. In addition, you might encounter the following workload-related situations:

- The throughput limit of the underlying instance type is reached.
- Queue depth is consistently less than 1 because your application isn't driving enough I/O operations.
- You experience query contention in the database even though some I/O capacity is unused.

In some cases, there isn't a system resource that is at or near a limit, and adding threads doesn't increase the database transaction rate. In such cases, the bottleneck is most likely contention in the database. The most common forms are row lock and index page lock contention, but there are many other possibilities. If this is your situation, seek the advice of a database performance tuning expert.

DB instance class

To get the most performance out of your Amazon RDS DB instance, choose a current generation instance type with enough bandwidth to support your storage type. For example, you can choose Amazon EBS-optimized instances and instances with 10-gigabit network connectivity.

Important

Depending on the instance class you're using, you might see lower IOPS performance than the maximum that you can provision with RDS. For specific information on IOPS performance for DB instance classes, see [Amazon EBS-optimized instances](#) in the *Amazon EC2 User Guide*.

We recommend that you determine the maximum IOPS for the instance class before setting a Provisioned IOPS value for your DB instance.

We encourage you to use the latest generation of instances to get the best performance. Previous generation DB instances can also have lower maximum storage.

Some older 32-bit file systems might have lower storage capacities. To determine the storage capacity of your DB instance, you can use the [describe-valid-db-instance-modifications](#) AWS CLI command.

The following list shows the maximum storage that most DB instance classes can scale to for each database engine:

- MariaDB – 64 TiB
- Microsoft SQL Server – 16 TiB
- MySQL – 64 TiB
- Oracle – 64 TiB
- PostgreSQL – 64 TiB

The following table shows some exceptions for maximum storage (in TiB). All RDS for Microsoft SQL Server DB instances have a maximum storage of 16 TiB, so there are no entries for SQL Server.

Instance class	MariaDB	MySQL	Oracle	PostgreSQL
db.m3 – standard instance classes				
db.m3.2xlarge	N/A	6	N/A	6
db.m3.xlarge	N/A	6	N/A	6
db.m3.large	N/A	6	N/A	6

Instance class	MariaDB	MySQL	Oracle	PostgreSQL
db.m3.medium	N/A	32	N/A	32
db.t4g – burstable-performance instance classes				
db.t4g.medium	16	16	N/A	32
db.t4g.small	16	16	N/A	16
db.t4g.micro	6	6	N/A	6
db.t3 – burstable-performance instance classes				
db.t3.medium	16	16	32	32
db.t3.small	16	16	32	16
db.t3.micro	6	6	32	6
db.t2 – burstable-performance instance classes				
db.t2.medium	32	32	N/A	32
db.t2.small	16	16	N/A	16
db.t2.micro	6	6	N/A	6

For more details about all instance classes supported, see [Previous generation DB instances](#).

Regions, Availability Zones, and Local Zones

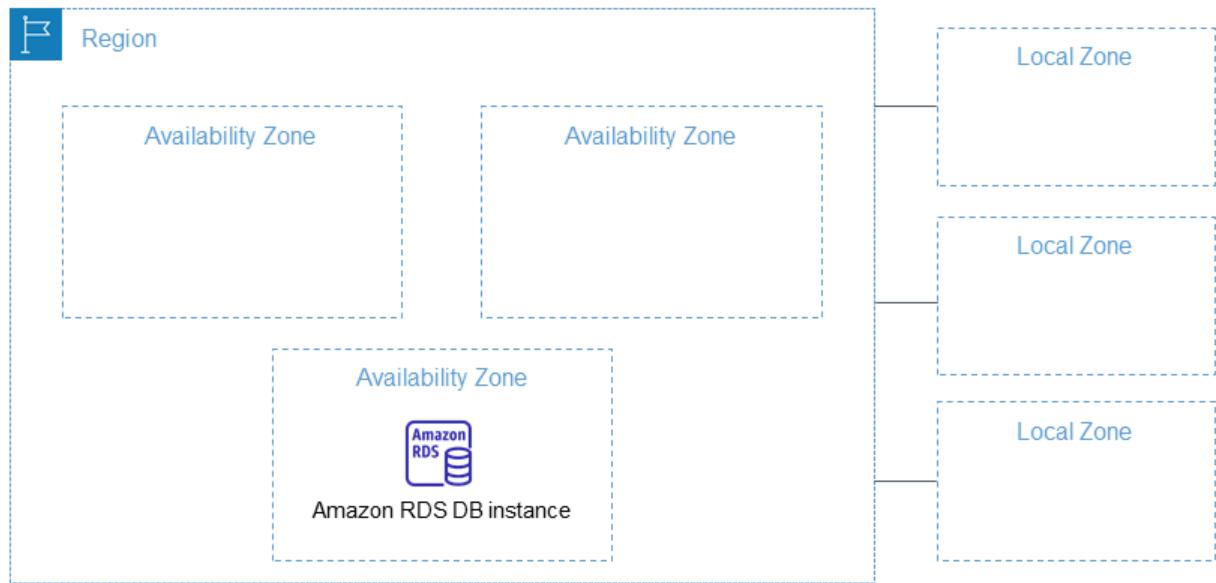
Amazon cloud computing resources are hosted in multiple locations world-wide. These locations are composed of AWS Regions, Availability Zones, and Local Zones. Each *AWS Region* is a separate geographic area. Each AWS Region has multiple, isolated locations known as *Availability Zones*.

Note

For information about finding the Availability Zones for an AWS Region, see [Describe your Availability Zones](#) in the Amazon EC2 documentation.

By using Local Zones, you can place resources, such as compute and storage, in multiple locations closer to your users. Amazon RDS enables you to place resources, such as DB instances, and data in multiple locations. Resources aren't replicated across AWS Regions unless you do so specifically.

Amazon operates state-of-the-art, highly-available data centers. Although rare, failures can occur that affect the availability of DB instances that are in the same location. If you host all your DB instances in one location that is affected by such a failure, none of your DB instances will be available.



It is important to remember that each AWS Region is completely independent. Any Amazon RDS activity you initiate (for example, creating database instances or listing available database instances) runs only in your current default AWS Region. The default AWS Region can be changed in the console, or by setting the `AWS_DEFAULT_REGION` environment variable. Or it can be overridden by using the `--region` parameter with the AWS Command Line Interface (AWS CLI). For more information, see [Configuring the AWS Command Line Interface](#), specifically the sections about environment variables and command line options.

Amazon RDS supports special AWS Regions called AWS GovCloud (US). These are designed to allow US government agencies and customers to move more sensitive workloads into the cloud. The AWS GovCloud (US) Regions address the US government's specific regulatory and compliance requirements. For more information, see [What is AWS GovCloud \(US\)?](#)

To create or work with an Amazon RDS DB instance in a specific AWS Region, use the corresponding regional service endpoint.

AWS Regions

Each AWS Region is designed to be isolated from the other AWS Regions. This design achieves the greatest possible fault tolerance and stability.

When you view your resources, you see only the resources that are tied to the AWS Region that you specified. This is because AWS Regions are isolated from each other, and we don't automatically replicate resources across AWS Regions.

Region availability

The following table shows the AWS Regions where Amazon RDS is currently available and the endpoint for each Region.

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS	
		rds-fips.us-east-2.api.aws	HTTPS	
		rds.us-east-2.api.aws	HTTPS	
		rds-fips.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS	
		rds-fips.us-east-1.api.aws	HTTPS	
		rds-fips.us-east-1.amazonaws.com	HTTPS	
		rds.us-east-1.api.aws	HTTPS	
US West (N. California)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS	
		rds.us-west-1.api.aws	HTTPS	
		rds-fips.us-west-1.amazonaws.com	HTTPS	
		rds-fips.us-west-1.api.aws	HTTPS	
US West (Oregon)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS	
		rds-fips.us-west-2.amazonaws.com	HTTPS	
		rds.us-west-2.api.aws	HTTPS	
		rds-fips.us-west-2.api.aws	HTTPS	
Africa (Cape Town)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
		rds.af-south-1.api.aws	HTTPS	
Asia Pacific (Hong Kong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
		rds.ap-east-1.api.aws	HTTPS	

Region Name	Region	Endpoint	Protocol	
Asia Pacific (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com rds.ap-south-1.api.aws	HTTPS HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com rds.ap-northeast-3.api.aws	HTTPS HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com rds.ap-northeast-2.api.aws	HTTPS HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com rds.ap-southeast-1.api.aws	HTTPS HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com rds.ap-southeast-2.api.aws	HTTPS HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com rds.ap-northeast-1.api.aws	HTTPS HTTPS	
Canada (Central)	ca-central-1	rds.ca-central-1.amazonaws.com rds.ca-central-1.api.aws rds-fips.ca-central-1.api.aws rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS HTTPS HTTPS	
Europe (Frankfurt)	eu-central-1	rds.eu-central-1.amazonaws.com rds.eu-central-1.api.aws	HTTPS HTTPS	
Europe (Ireland)	eu-west-1	rds.eu-west-1.amazonaws.com rds.eu-west-1.api.aws	HTTPS HTTPS	
Europe (London)	eu-west-2	rds.eu-west-2.amazonaws.com rds.eu-west-2.api.aws	HTTPS HTTPS	
Europe (Milan)	eu-south-1	rds.eu-south-1.amazonaws.com rds.eu-south-1.api.aws	HTTPS HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com rds.eu-west-3.api.aws	HTTPS HTTPS	
Europe (Spain)	eu-south-2	rds.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com rds.eu-north-1.api.aws	HTTPS HTTPS	
Europe (Zurich)	eu-central-2	rds.eu-central-2.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	rds.me-south-1.amazonaws.com rds.me-south-1.api.aws	HTTPS HTTPS	
Middle East (UAE)	me-central-1	rds.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com rds.sa-east-1.api.aws	HTTPS HTTPS	
AWS GovCloud (US-East)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-West)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com	HTTPS	

If you do not explicitly specify an endpoint, the US West (Oregon) endpoint is the default.

When you work with a DB instance using the AWS CLI or API operations, make sure that you specify its regional endpoint.

Availability Zones

When you create a DB instance, you can choose an Availability Zone or have Amazon RDS choose one for you randomly. An Availability Zone is represented by an AWS Region code followed by a letter identifier (for example, us-east-1a).

You can't choose the Availability Zones for the primary and secondary DB instances in a Multi-AZ DB deployment. Amazon RDS chooses them for you randomly. For more information about Multi-AZ deployments, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Note

Random selection of Availability Zones by RDS doesn't guarantee an even distribution of DB instances among Availability Zones within a single account or DB subnet group. You can request a specific AZ when you create or modify a Single-AZ instance, and you can use more-specific DB subnet groups for Multi-AZ instances. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#) and [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Local Zones

A *Local Zone* is an extension of an AWS Region that is geographically close to your users. You can extend any VPC from the parent AWS Region into Local Zones. To do so, create a new subnet and assigning it to the AWS Local Zone. When you create a subnet in a Local Zone, your VPC is extended to that Local Zone. The subnet in the Local Zone operates the same as other subnets in your VPC.

When you create a DB instance, you can choose a subnet in a Local Zone. Local Zones have their own connections to the internet and support AWS Direct Connect. Thus, resources created in a Local Zone can serve local users with very low-latency communications. For more information, see [AWS Local Zones](#).

A Local Zone is represented by an AWS Region code followed by an identifier that indicates the location, for example us-west-2-lax-1a.

Note

A Local Zone can't be included in a Multi-AZ deployment.

To use a Local Zone

1. Enable the Local Zone in the Amazon EC2 console.

For more information, see [Enabling Local Zones in the Amazon EC2 User Guide for Linux Instances](#).

2. Create a subnet in the Local Zone.

For more information, see [Creating a subnet in your VPC](#) in the *Amazon VPC User Guide*.

3. Create a DB subnet group in the Local Zone.

When you create a DB subnet group, choose the Availability Zone group for the Local Zone.

For more information, see [Creating a DB instance in a VPC \(p. 2111\)](#).

4. Create a DB instance that uses the DB subnet group in the Local Zone.

For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Important

Currently, the only AWS Local Zone where Amazon RDS is available is Los Angeles in the US West (Oregon) Region.

Supported features in Amazon RDS by AWS Region and DB engine

Support for Amazon RDS features and options varies across AWS Regions and specific versions of each DB engine. To identify RDS DB engine version support and availability in a given AWS Region, you can use the following sections.

Amazon RDS features are different from engine-native features and options. For more information on engine-native features and options, see [Engine-native features. \(p. 120\)](#)

Topics

- [Table conventions \(p. 77\)](#)
- [Feature quick reference \(p. 77\)](#)
- [Cross-Region automated backups \(p. 78\)](#)
- [Cross-Region read replicas \(p. 83\)](#)
- [Database activity streams \(p. 85\)](#)
- [Dual-stack mode \(p. 88\)](#)
- [Export snapshots to S3 \(p. 95\)](#)
- [IAM database authentication \(p. 99\)](#)
- [Kerberos authentication \(p. 101\)](#)
- [Multi-AZ DB clusters \(p. 107\)](#)
- [Performance Insights \(p. 110\)](#)
- [RDS Custom \(p. 110\)](#)
- [Amazon RDS Proxy \(p. 114\)](#)
- [Engine-native features \(p. 120\)](#)

Table conventions

The tables in the feature sections use these patterns to specify version numbers and level of support:

- **Version x.y** – The specific version alone is supported.
- **Version x.y and higher** – The version and all higher minor versions are supported. For example, "version 10.11 and higher" means that versions 10.11, 10.11.1, and 10.12 are supported.
- – – The feature isn't currently available for that particular RDS feature for the given RDS DB engine, or in that specific AWS Region.

Feature quick reference

The following quick reference table lists each feature and supported RDS DB engine. Region and specific version availability appears in the later feature sections.

Feature	RDS for MariaDB	RDS for MySQL	RDS for Oracle	RDS for PostgreSQL	RDS for SQL Server
Cross-Region	–	–	Available (p. 79)	Available (p. 80)	Available (p. 82)

Feature	RDS for MariaDB	RDS for MySQL	RDS for Oracle	RDS for PostgreSQL	RDS for SQL Server
automated backups					
Cross-Region read replicas	Available (p. 84)				
Database activity streams	–	–	Available (p. 85)	–	–
Dual-stack mode	Available (p. 88)	Available (p. 90)	Available (p. 91)	Available (p. 92)	Available (p. 93)
Export Snapshot to Amazon S3	Available (p. 95)	Available (p. 96)	–	Available (p. 97)	–
AWS Identity and Access Management (IAM) database authentication	Available (p. 99)	Available (p. 101)	–	Available (p. 101)	–
Kerberos authentication	–	Available (p. 102)	Available (p. 103)	Available (p. 104)	Available (p. 106)
Multi-AZ DB clusters	–	Available (p. 107)	–	Available (p. 109)	–
Performance Insights	Available (p. 110)				
RDS Custom	–	–	Available (p. 111)	–	Available (p. 113)
RDS Proxy	Available (p. 115)	Available (p. 116)	–	Available (p. 117)	Available (p. 119)

Cross-Region automated backups

By using backup replication in Amazon RDS, you can configure your RDS DB instance to replicate snapshots and transaction logs to a destination Region. When backup replication is configured for a DB instance, RDS starts a cross-Region copy of all snapshots and transaction logs when they're ready. For more information, see [Replicating automated backups to another AWS Region \(p. 437\)](#).

Backup replication isn't available with the following engines:

- RDS for MariaDB
- RDS for MySQL

For more information on limitations for source and destination backup Regions, see [Replicating automated backups to another AWS Region \(p. 437\)](#).

Topics

- [Backup replication with RDS for Oracle \(p. 79\)](#)
- [Backup replication with RDS for PostgreSQL \(p. 80\)](#)
- [Backup replication with RDS for SQL Server \(p. 82\)](#)

Backup replication with RDS for Oracle

Following are the supported engines and Region availability for backup replication with RDS for Oracle.

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
US East (Ohio)	All versions	All versions	Version 12.1.0.2.v10 and higher
US East (N. Virginia)	All versions	All versions	Version 12.1.0.2.v10 and higher
US West (N. California)	All versions	All versions	Version 12.1.0.2.v10 and higher
US West (Oregon)	All versions	All versions	Version 12.1.0.2.v10 and higher
Africa (Cape Town)	–	–	–
Asia Pacific (Hong Kong)	–	–	–
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	Version 12.1.0.2.v10 and higher
Asia Pacific (Osaka)	All versions	All versions	Version 12.1.0.2.v10 and higher
Asia Pacific (Seoul)	All versions	All versions	Version 12.1.0.2.v10 and higher
Asia Pacific (Singapore)	All versions	All versions	Version 12.1.0.2.v10 and higher
Asia Pacific (Sydney)	All versions	All versions	Version 12.1.0.2.v10 and higher
Asia Pacific (Tokyo)	All versions	All versions	Version 12.1.0.2.v10 and higher
Canada (Central)	All versions	All versions	Version 12.1.0.2.v10 and higher

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
China (Beijing)	All versions	All versions	Version 12.1.0.2.v10 and higher
China (Ningxia)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (Frankfurt)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (Ireland)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (London)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (Milan)	–	–	–
Europe (Paris)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	Version 12.1.0.2.v10 and higher
Europe (Zurich)	–	–	–
Middle East (Bahrain)	All versions	All versions	Version 12.1.0.2.v10 and higher
Middle East (UAE)	All versions	All versions	Version 12.1.0.2.v10 and higher
South America (São Paulo)	All versions	All versions	Version 12.1.0.2.v10 and higher
AWS GovCloud (US-East)	All versions	All versions	Version 12.1.0.2.v10 and higher
AWS GovCloud (US-West)	All versions	All versions	Version 12.1.0.2.v10 and higher

Backup replication with RDS for PostgreSQL

Following are the supported engines and Region availability for backup replication with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US East (Ohio)	All versions				
US East (N. Virginia)	All versions				

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US West (N. California)	All versions				
US West (Oregon)	All versions				
Africa (Cape Town)	–	–	–	–	–
Asia Pacific (Hong Kong)	–	–	–	–	–
Asia Pacific (Hyderabad)	–	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–	–
Asia Pacific (Mumbai)	All versions				
Asia Pacific (Osaka)	All versions				
Asia Pacific (Seoul)	All versions				
Asia Pacific (Singapore)	All versions				
Asia Pacific (Sydney)	All versions				
Asia Pacific (Tokyo)	All versions				
Canada (Central)	All versions				
China (Beijing)	All versions				
China (Ningxia)	All versions				
Europe (Frankfurt)	All versions				
Europe (Ireland)	All versions				
Europe (London)	All versions				
Europe (Milan)	–	–	–	–	–
Europe (Paris)	All versions				
Europe (Spain)	–	–	–	–	–
Europe (Stockholm)	All versions				

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
Europe (Zurich)	–	–	–	–	–
Middle East (Bahrain)	All versions				
Middle East (UAE)	All versions	All versions	All versions	All versions	
South America (São Paulo)	All versions				
AWS GovCloud (US-East)	All versions				
AWS GovCloud (US-West)	All versions				

Backup replication with RDS for SQL Server

Following are the supported engines and Region availability for backup replication with RDS for SQL Server.

Note

Backup replication isn't supported for encrypted SQL Server DB instances. Make sure to clear the **Enable encryption** check box when you create a SQL Server DB instance for which you want to use backup replication.

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
US East (Ohio)	All versions	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions	All versions
Africa (Cape Town)	–	–	–	–
Asia Pacific (Hong Kong)	–	–	–	–
Asia Pacific (Hyderabad)	–	–	–	
Asia Pacific (Jakarta)	–	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions	All versions

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
Asia Pacific (Singapore)	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions	All versions
Europe (Milan)	–	–	–	–
Europe (Paris)	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions	All versions
Middle East (UAE)	All versions	All versions	All versions	All versions
South America (São Paulo)	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions	All versions
AWS GovCloud (US-West)	All versions	All versions	All versions	All versions

Cross-Region read replicas

By using cross-Region read replicas in Amazon RDS, you can create a MariaDB, MySQL, Oracle, PostgreSQL, or SQL Server read replica in a different Region from the source DB instance. For more information about cross-Region read replicas, including source and destination Region considerations, see [Creating a read replica in a different AWS Region \(p. 383\)](#).

Topics

- [Cross-Region read replicas with RDS for MariaDB \(p. 84\)](#)
- [Cross-Region read replicas with RDS for MySQL \(p. 84\)](#)
- [Cross-Region read replicas with RDS for Oracle \(p. 84\)](#)
- [Cross-Region read replicas with RDS for PostgreSQL \(p. 84\)](#)
- [Cross-Region read replicas with RDS for SQL Server \(p. 84\)](#)

Cross-Region read replicas with RDS for MariaDB

Cross-Region read replicas with RDS for MariaDB are available in all Regions for the following versions:

- RDS for MariaDB 10.6 (All versions)
- RDS for MariaDB 10.5 (All versions)
- RDS for MariaDB 10.4 (All versions)
- RDS for MariaDB 10.3 (All versions)

Cross-Region read replicas with RDS for MySQL

Cross-Region read replicas with RDS for MySQL are available in all Regions for the following versions:

- RDS for MySQL 8.0 (All versions)
- RDS for MySQL 5.7 (All versions)

Cross-Region read replicas with RDS for Oracle

Cross-Region read replicas for RDS for Oracle are available in all Regions with the following version limitations:

- For RDS for Oracle 21c, cross-Region read replicas aren't available.
- For RDS for Oracle 19c, cross-Region read replicas are available for instances of Oracle Database 19c that aren't container database (CBD) instances.
- For RDS for Oracle 12c, cross-Region read replicas are available for Oracle Enterprise Edition (EE) of Oracle Database 12c Release 1 (12.1) using 12.1.0.2.v10 and higher 12c releases.

For more information on additional requirements for cross-Region read replicas with RDS for Oracle, see [Considerations for RDS for Oracle replicas \(p. 1631\)](#).

Cross-Region read replicas with RDS for PostgreSQL

Cross-Region read replicas with RDS for PostgreSQL are available in all Regions for the following versions:

- RDS for PostgreSQL 14 (All versions)
- RDS for PostgreSQL 13 (All versions)
- RDS for PostgreSQL 12 (All versions)
- RDS for PostgreSQL 11 (All versions)
- RDS for PostgreSQL 10 (All versions)

Cross-Region read replicas with RDS for SQL Server

Cross-Region read replicas with RDS for SQL Server are available in all Regions except the following:

- Africa (Cape Town)
- Asia Pacific (Jakarta)
- Asia Pacific (Hong Kong)
- China (Beijing)

- China (Ningxia)
- Europe (Milan)
- Middle East (Bahrain)
- Middle East (UAE)

Cross-Region read replicas with RDS for SQL Server are available for the following versions using Microsoft SQL Server Enterprise Edition:

- RDS for SQL Server 2019 (Version 15.00.4073.23 and higher)
- RDS for SQL Server 2017 (Version 14.00.3049.1 and higher)
- RDS for SQL Server 2016 (Version 13.00.5216.0 and higher)

Database activity streams

By using Database Activity Streams in Amazon RDS, you can monitor and set alarms for auditing activity in your Oracle database. For more information, see [Overview of Database Activity Streams \(p. 729\)](#).

Database activity streams aren't available with the following engines:

- RDS for MariaDB
- RDS for MySQL
- RDS for PostgreSQL
- RDS for SQL Server

Topics

- [Database activity streams with RDS for Oracle \(p. 85\)](#)

Database activity streams with RDS for Oracle

Following are the supported engines and Region availability for database activity streams with RDS for Oracle.

For more information on additional requirements for database activity streams with RDS for Oracle, see [Overview of Database Activity Streams \(p. 729\)](#).

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
US East (Ohio)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
US East (N. Virginia)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
US West (N. California)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either	–

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
		Enterprise Edition (EE) or Standard Edition 2 (SE2)	
US West (Oregon)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Africa (Cape Town)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Hong Kong)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Mumbai)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Osaka)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Seoul)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Singapore)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
Asia Pacific (Sydney)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Asia Pacific (Tokyo)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Canada (Central)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
China (Beijing)	–	–	–
China (Ningxia)	–	–	–
Europe (Frankfurt)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (Ireland)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (London)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (Milan)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (Paris)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (Spain)	–	–	–

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
Europe (Stockholm)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Europe (Zurich)	–	–	–
Middle East (Bahrain)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
Middle East (UAE)	–	–	–
South America (São Paulo)	–	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 and higher, using either Enterprise Edition (EE) or Standard Edition 2 (SE2)	–
AWS GovCloud (US-East)	–	–	–
AWS GovCloud (US-West)	–	–	–

Dual-stack mode

By using dual-stack mode in RDS, resources can communicate with a DB instance over Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), or both. For more information, see [Dual-stack mode \(p. 2106\)](#).

Topics

- [Dual-stack mode with RDS for MariaDB \(p. 88\)](#)
- [Dual-stack mode with RDS for MySQL \(p. 90\)](#)
- [Dual-stack mode with RDS for Oracle \(p. 91\)](#)
- [Dual-stack mode with RDS for PostgreSQL \(p. 92\)](#)
- [Dual-stack mode with RDS for SQL Server \(p. 93\)](#)

Dual-stack mode with RDS for MariaDB

Following are the supported engines and Region availability for dual-stack mode with RDS for MariaDB.

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US East (Ohio)	All versions	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions	All versions

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US West (N. California)	All versions	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–	–
Asia Pacific (Jakarta)	All versions	All versions	All versions	All versions
Asia Pacific (Mumbai)	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions	All versions
Middle East (UAE)	–	–	–	–
South America (São Paulo)	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions	All versions

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
AWS GovCloud (US-West)	All versions	All versions	All versions	All versions

Dual-stack mode with RDS for MySQL

Following are the supported engines and Region availability for dual-stack mode with RDS for MySQL.

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	All versions	All versions	All versions
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
Europe (Zurich)	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions
AWS GovCloud (US-West)	All versions	All versions	All versions

Dual-stack mode with RDS for Oracle

Following are the supported engines and Region availability for dual-stack mode with RDS for Oracle.

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	All versions	All versions	All versions
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
Europe (Paris)	All versions	All versions	All versions
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions
Europe (Zurich)	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions
AWS GovCloud (US-West)	All versions	All versions	All versions

Dual-stack mode with RDS for PostgreSQL

Following are the supported engines and Region availability for dual-stack mode with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US East (Ohio)	All versions				
US East (N. Virginia)	All versions				
US West (N. California)	All versions				
US West (Oregon)	All versions				
Africa (Cape Town)	All versions				
Asia Pacific (Hong Kong)	All versions				
Asia Pacific (Hyderabad)	–	–	–	–	–
Asia Pacific (Jakarta)	All versions				
Asia Pacific (Mumbai)	All versions				
Asia Pacific (Osaka)	All versions				
Asia Pacific (Seoul)	All versions				

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
Asia Pacific (Singapore)	All versions				
Asia Pacific (Sydney)	All versions				
Asia Pacific (Tokyo)	All versions				
Canada (Central)	All versions				
China (Beijing)	All versions				
China (Ningxia)	All versions				
Europe (Frankfurt)	All versions				
Europe (Ireland)	All versions				
Europe (London)	All versions				
Europe (Milan)	All versions				
Europe (Paris)	All versions				
Europe (Spain)	–	–	–	–	–
Europe (Stockholm)	All versions				
Europe (Zurich)	–	–	–	–	–
Middle East (Bahrain)	All versions				
Middle East (UAE)	–	–	–	–	–
South America (São Paulo)	All versions				
AWS GovCloud (US-East)	All versions				
AWS GovCloud (US-West)	All versions				

Dual-stack mode with RDS for SQL Server

Following are the supported engines and Region availability for dual-stack mode with RDS for SQL Server.

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
US East (Ohio)	All versions	All versions	All versions	–
US East (N. Virginia)	All versions	All versions	All versions	–
US West (N. California)	All versions	All versions	All versions	–
US West (Oregon)	All versions	All versions	All versions	–
Africa (Cape Town)	All versions	All versions	All versions	–
Asia Pacific (Hong Kong)	All versions	All versions	All versions	–
Asia Pacific (Hyderabad)	–	–	–	–
Asia Pacific (Jakarta)	All versions	All versions	All versions	–
Asia Pacific (Mumbai)	All versions	All versions	All versions	–
Asia Pacific (Osaka)	All versions	All versions	All versions	–
Asia Pacific (Seoul)	All versions	All versions	All versions	–
Asia Pacific (Singapore)	All versions	All versions	All versions	–
Asia Pacific (Sydney)	All versions	All versions	All versions	–
Asia Pacific (Tokyo)	All versions	All versions	All versions	–
Canada (Central)	All versions	All versions	All versions	–
China (Beijing)	All versions	All versions	All versions	–
China (Ningxia)	All versions	All versions	All versions	–
Europe (Frankfurt)	All versions	All versions	All versions	–
Europe (Ireland)	All versions	All versions	All versions	–
Europe (London)	All versions	All versions	All versions	–
Europe (Milan)	All versions	All versions	All versions	–
Europe (Paris)	All versions	All versions	All versions	–
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	–
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions	–
Middle East (UAE)	–	–	–	–

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
South America (São Paulo)	All versions	All versions	All versions	—
AWS GovCloud (US-East)	All versions	All versions	All versions	—
AWS GovCloud (US-West)	All versions	All versions	All versions	—

Export snapshots to S3

You can export RDS DB snapshot data to an Amazon S3 bucket. You can export all types of DB snapshots—including manual snapshots, automated system snapshots, and snapshots created by AWS Backup. After the data is exported, you can analyze the exported data directly through tools like Amazon Athena or Amazon Redshift Spectrum. For more information, see [Exporting DB snapshot data to Amazon S3 \(p. 481\)](#).

Topics

- [Export snapshots to S3 with RDS for MariaDB \(p. 95\)](#)
- [Export snapshots to S3 with RDS for MySQL \(p. 96\)](#)
- [Export snapshots to S3 with RDS for PostgreSQL \(p. 97\)](#)

Export snapshots to S3 with RDS for MariaDB

Following are the supported engines and Region availability for exporting snapshots to S3 with RDS for MariaDB.

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US East (Ohio)	All versions	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions	All versions
Asia Pacific (Hyderabad)	—	—	—	—
Asia Pacific (Jakarta)	—	—	—	—
Asia Pacific (Mumbai)	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions	All versions

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
Asia Pacific (Seoul)	All versions	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions	All versions
Middle East (UAE)	–	–	–	–
South America (São Paulo)	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–

Export snapshots to S3 with RDS for MySQL

Following are the supported engines and Region availability for exporting snapshots to S3 with RDS for MySQL.

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions
Europe (Zurich)	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–
AWS GovCloud (US-West)	–	–	–

Export snapshots to S3 with RDS for PostgreSQL

Following are the supported engines and Region availability for exporting snapshots to S3 with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US East (Ohio)	All versions				
US East (N. Virginia)	All versions				
US West (N. California)	All versions				
US West (Oregon)	All versions				
Africa (Cape Town)	All versions				
Asia Pacific (Hong Kong)	All versions				
Asia Pacific (Hyderabad)	–	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–	–
Asia Pacific (Mumbai)	All versions				
Asia Pacific (Osaka)	All versions				
Asia Pacific (Seoul)	All versions				
Asia Pacific (Singapore)	All versions				
Asia Pacific (Sydney)	All versions				
Asia Pacific (Tokyo)	All versions				
Canada (Central)	All versions				
China (Beijing)	All versions				
China (Ningxia)	All versions				
Europe (Frankfurt)	All versions				
Europe (Ireland)	All versions				
Europe (London)	All versions				
Europe (Milan)	All versions				
Europe (Paris)	All versions				

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
Europe (Spain)	–	–	–	–	–
Europe (Stockholm)	All versions				
Europe (Zurich)	–	–	–	–	–
Middle East (Bahrain)	All versions				
Middle East (UAE)	–	–	–	–	–
South America (São Paulo)	All versions				
AWS GovCloud (US-East)	–	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–	–

IAM database authentication

By using IAM database authentication in Amazon RDS, you can authenticate without a password when you connect to a DB instance. Instead, you use an authentication token. For more information, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

IAM database authentication isn't available with the following engines:

- RDS for Oracle
- RDS for SQL Server

Topics

- [IAM database authentication with RDS for MariaDB \(p. 99\)](#)
- [IAM database authentication with RDS for MySQL \(p. 101\)](#)
- [IAM database authentication with RDS for PostgreSQL \(p. 101\)](#)

IAM database authentication with RDS for MariaDB

Following are the supported engines and Region availability for IAM database authentication with RDS for MariaDB.

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US East (Ohio)	Version 10.6 and higher	-	-	-
US East (N. Virginia)	Version 10.6 and higher	-	-	-

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US West (N. California)	Version 10.6 and higher	-	-	-
US West (Oregon)	Version 10.6 and higher	-	-	-
Africa (Cape Town)	Version 10.6 and higher	-	-	-
Asia Pacific (Hong Kong)	Version 10.6 and higher	-	-	-
Asia Pacific (Hyderabad)	-	-	-	-
Asia Pacific (Jakarta)	Version 10.6 and higher	-	-	-
Asia Pacific (Mumbai)	Version 10.6 and higher	-	-	-
Asia Pacific (Osaka)	Version 10.6 and higher	-	-	-
Asia Pacific (Seoul)	Version 10.6 and higher	-	-	-
Asia Pacific (Singapore)	Version 10.6 and higher	-	-	-
Asia Pacific (Sydney)	Version 10.6 and higher	-	-	-
Asia Pacific (Tokyo)	Version 10.6 and higher	-	-	-
Canada (Central)	Version 10.6 and higher	-	-	-
China (Beijing)	Version 10.6 and higher	-	-	-
China (Ningxia)	Version 10.6 and higher	-	-	-
Europe (Frankfurt)	Version 10.6 and higher	-	-	-
Europe (Ireland)	Version 10.6 and higher	-	-	-
Europe (London)	Version 10.6 and higher	-	-	-
Europe (Milan)	Version 10.6 and higher	-	-	-

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
Europe (Paris)	Version 10.6 and higher	-	-	-
Europe (Spain)	-	-	-	-
Europe (Stockholm)	Version 10.6 and higher	-	-	-
Europe (Zurich)	-	-	-	-
Middle East (Bahrain)	Version 10.6 and higher	-	-	-
Middle East (UAE)	-	-	-	-
South America (São Paulo)	Version 10.6 and higher	-	-	-
AWS GovCloud (US-East)	Version 10.6 and higher	-	-	-
AWS GovCloud (US-West)	Version 10.6 and higher	-	-	-

IAM database authentication with RDS for MySQL

IAM database authentication with RDS for MySQL is available in all Regions for the following versions:

- RDS for MySQL 8.0 (All versions)
- RDS for MySQL 5.7 (All versions)
- RDS for MySQL 5.6 (All versions)

IAM database authentication with RDS for PostgreSQL

IAM database authentication with RDS for PostgreSQL is available in all Regions for the following versions:

- RDS for PostgreSQL 14 (All versions)
- RDS for PostgreSQL 13 (All versions)
- RDS for PostgreSQL 12 (All versions)
- RDS for PostgreSQL 11 (All versions)
- RDS for PostgreSQL 10 (All versions)

Kerberos authentication

By using Kerberos authentication in Amazon RDS, you can support external authentication of database users using Kerberos and Microsoft Active Directory. Using Kerberos and Active Directory provides the benefits of single sign-on and centralized authentication of database users. For more information, see [Kerberos authentication \(p. 1999\)](#).

Kerberos authentication isn't available with the following engines:

- RDS for MariaDB

Topics

- [Kerberos authentication with RDS for MySQL \(p. 102\)](#)
- [Kerberos authentication with RDS for Oracle \(p. 103\)](#)
- [Kerberos authentication with RDS for PostgreSQL \(p. 104\)](#)
- [Kerberos authentication with RDS for SQL Server \(p. 106\)](#)

Kerberos authentication with RDS for MySQL

Following are the supported engines and Region availability for Kerberos authentication with RDS for MySQL.

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	–	–	–
Asia Pacific (Hong Kong)	–	–	–
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	–	–	–
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	–	–	–
Europe (Paris)	–	–	–

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions
Europe (Zurich)	–	–	–
Middle East (Bahrain)	–	–	–
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–
AWS GovCloud (US-West)	–	–	–

Kerberos authentication with RDS for Oracle

Following are the supported engines and Region availability for Kerberos authentication with RDS for Oracle.

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	–	–	–
Asia Pacific (Hong Kong)	–	–	–
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	–	–	–
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	–	–	–
China (Ningxia)	–	–	–
Europe (Frankfurt)	All versions	All versions	All versions

Region	RDS for Oracle 21c	RDS for Oracle 19c	RDS for Oracle 12c
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	–	–	–
Europe (Paris)	–	–	–
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions
Europe (Zurich)	–	–	–
Middle East (Bahrain)	–	–	–
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions
AWS GovCloud (US-West)	All versions	All versions	All versions

Kerberos authentication with RDS for PostgreSQL

Following are the supported engines and Region availability for Kerberos authentication with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US East (Ohio)	All versions				
US East (N. Virginia)	All versions				
US West (N. California)	All versions				
US West (Oregon)	All versions				
Africa (Cape Town)	–	–	–	–	–
Asia Pacific (Hong Kong)	–	–	–	–	–
Asia Pacific (Hyderabad)	–	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–	–
Asia Pacific (Mumbai)	All versions				

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
Asia Pacific (Osaka)	–	–	–	–	–
Asia Pacific (Seoul)	All versions				
Asia Pacific (Singapore)	All versions				
Asia Pacific (Sydney)	All versions				
Asia Pacific (Tokyo)	All versions				
Canada (Central)	All versions				
China (Beijing)	All versions				
China (Ningxia)	All versions				
Europe (Frankfurt)	All versions				
Europe (Ireland)	All versions				
Europe (London)	All versions				
Europe (Milan)	–	–	–	–	–
Europe (Paris)	All versions				
Europe (Spain)	–	–	–	–	–
Europe (Stockholm)	All versions				
Europe (Zurich)	–	–	–	–	–
Middle East (Bahrain)	–	–	–	–	–
Middle East (UAE)	–	–	–	–	–
South America (São Paulo)	All versions				
AWS GovCloud (US-East)	All versions				
AWS GovCloud (US-West)	All versions				

Kerberos authentication with RDS for SQL Server

Following are the supported engines and Region availability for Kerberos authentication with RDS for SQL Server.

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
US East (Ohio)	All versions	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–	–
Asia Pacific (Jakarta)	All versions	All versions	All versions	All versions
Asia Pacific (Mumbai)	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions	All versions
China (Beijing)	All versions	All versions	All versions	All versions
China (Ningxia)	All versions	All versions	All versions	All versions
Europe (Frankfurt)	All versions	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
Middle East (Bahrain)	All versions	All versions	All versions	All versions
Middle East (UAE)	–	–	–	–
South America (São Paulo)	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	All versions	All versions	All versions	All versions
AWS GovCloud (US-West)	All versions	All versions	All versions	All versions

Multi-AZ DB clusters

A Multi-AZ DB cluster deployment in Amazon RDS provides a high availability deployment mode of Amazon RDS with two readable standby DB instances. A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same Region. Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower write latency when compared to Multi-AZ DB instance deployments. For more information, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

Multi-AZ DB clusters aren't available with the following engines:

- RDS for MariaDB
- RDS for Oracle
- RDS for SQL Server

Topics

- [Multi-AZ DB clusters with RDS for MySQL \(p. 107\)](#)
- [Multi-AZ DB clusters with RDS for PostgreSQL \(p. 109\)](#)

Multi-AZ DB clusters with RDS for MySQL

Following are the supported engines and Region availability for Multi-AZ DB clusters with RDS for MySQL.

Region	RDS for MySQL 8.0
US East (Ohio)	Version 8.0.28 and higher
US East (N. Virginia)	Version 8.0.28 and higher
US West (N. California)	–
US West (Oregon)	Version 8.0.28 and higher
Africa (Cape Town)	Version 8.0.28 and higher
Asia Pacific (Hong Kong)	Version 8.0.28 and higher

Region	RDS for MySQL 8.0
Asia Pacific (Hyderabad)	–
Asia Pacific (Jakarta)	Version 8.0.28 and higher
Asia Pacific (Mumbai)	Version 8.0.28 and higher
Asia Pacific (Osaka)	Version 8.0.28 and higher
Asia Pacific (Seoul)	Version 8.0.28 and higher
Asia Pacific (Singapore)	Version 8.0.28 and higher
Asia Pacific (Sydney)	Version 8.0.28 and higher
Asia Pacific (Tokyo)	Version 8.0.28 and higher
Canada (Central)	Version 8.0.28 and higher
China (Beijing)	–
China (Ningxia)	–
Europe (Frankfurt)	Version 8.0.28 and higher
Europe (Ireland)	Version 8.0.28 and higher
Europe (London)	Version 8.0.28 and higher
Europe (Milan)	Version 8.0.28 and higher
Europe (Paris)	Version 8.0.28 and higher
Europe (Spain)	–
Europe (Stockholm)	Version 8.0.28 and higher
Europe (Zurich)	–
Middle East (Bahrain)	Version 8.0.28 and higher
Middle East (UAE)	–
South America (São Paulo)	Version 8.0.28 and higher
AWS GovCloud (US-East)	–
AWS GovCloud (US-West)	–

You can also list the supported versions in a Region for the db.r5d.large DB instance class by running the following AWS CLI command.

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options \
--engine mysql \
--db-instance-class db.r5d.large \
--query '*[]|[?SupportsClusters == `true`].[EngineVersion]' \
--output text
```

For Windows:

```
aws rds describe-orderable-db-instance-options ^
--engine mysql ^
--db-instance-class db.r5d.large ^
--query "[*[]|[?SupportsClusters == `true`].[EngineVersion]]" ^
--output text
```

You can change the DB instance class to show the supported engine versions for it.

Multi-AZ DB clusters with RDS for PostgreSQL

Following are the supported engine version and Region availability for Multi-AZ DB clusters with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13
US East (Ohio)	Version 14.5	Version 13.4 and version 13.7
US East (N. Virginia)	Version 14.5	Version 13.4 and version 13.7
US West (N. California)	–	–
US West (Oregon)	Version 14.5	Version 13.4 and version 13.7
Africa (Cape Town)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Hong Kong)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Hyderabad)	–	–
Asia Pacific (Jakarta)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Mumbai)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Osaka)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Seoul)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Singapore)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Sydney)	Version 14.5	Version 13.4 and version 13.7
Asia Pacific (Tokyo)	Version 14.5	Version 13.4 and version 13.7
Canada (Central)	Version 14.5	Version 13.4 and version 13.7
China (Beijing)	–	–
China (Ningxia)	–	–
Europe (Frankfurt)	Version 14.5	Version 13.4 and version 13.7
Europe (Ireland)	Version 14.5	Version 13.4 and version 13.7
Europe (London)	Version 14.5	Version 13.4 and version 13.7
Europe (Milan)	Version 14.5	Version 13.4 and version 13.7
Europe (Paris)	Version 14.5	Version 13.4 and version 13.7
Europe (Spain)	–	–

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13
Europe (Stockholm)	Version 14.5	Version 13.4 and version 13.7
Europe (Zurich)	–	–
Middle East (Bahrain)	Version 14.5	Version 13.4 and version 13.7
Middle East (UAE)	–	–
South America (São Paulo)	Version 14.5	Version 13.4 and version 13.7
AWS GovCloud (US-East)	–	–
AWS GovCloud (US-West)	–	–

You can also list the supported versions in a Region for the db.r5d.large DB instance class by running the following AWS CLI command.

For Linux, macOS, or Unix:

```
aws rds describe-orderable-db-instance-options \
--engine postgres \
--db-instance-class db.r5d.large \
--query '*[]|[?SupportsClusters == `true`].[EngineVersion]' \
--output text
```

For Windows:

```
aws rds describe-orderable-db-instance-options ^
--engine postgres ^
--db-instance-class db.r5d.large ^
--query "*[]|[?SupportsClusters == `true`].[EngineVersion]" ^
--output text
```

You can change the DB instance class to show the supported engine versions for it.

Performance Insights

Performance Insights in Amazon RDS expands on existing Amazon RDS monitoring features to illustrate and help you analyze your database performance. With the Performance Insights dashboard, you can visualize the database load on your Amazon RDS DB instance. You can also filter the load by waits, SQL statements, hosts, or users. For more information, see [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#).

Performance Insights is available for all RDS DB engines and all versions.

Performance Insights is available in all AWS Regions except the following:

- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

RDS Custom

Amazon RDS Custom automates database administration tasks and operations. By using RDS Custom, as a database administrator you can access and customize your database environment and operating

system. With RDS Custom, you can customize to meet the requirements of legacy, custom, and packaged applications. For more information, see [Working with Amazon RDS Custom \(p. 755\)](#).

RDS Custom isn't available with the following engines:

- RDS for MariaDB
- RDS for MySQL
- RDS for PostgreSQL

Topics

- [RDS Custom with RDS for Oracle \(p. 111\)](#)
- [RDS Custom with RDS for SQL Server \(p. 113\)](#)

RDS Custom with RDS for Oracle

Following are the supported engine versions and Region availability for RDS Custom with RDS for Oracle.

Region	RDS for Oracle 19c	RDS for Oracle 18c	RDS for Oracle 12c
US East (Ohio)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
US East (N. Virginia)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
US West (N. California)	–	–	–
US West (Oregon)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Africa (Cape Town)	–	–	–
Asia Pacific (Hong Kong)	–	–	–
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	19c with the January	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR

Region	RDS for Oracle 19c	RDS for Oracle 18c	RDS for Oracle 12c
	2021 or higher RU/RUR		
Asia Pacific (Osaka)	–	–	–
Asia Pacific (Seoul)	–	–	–
Asia Pacific (Singapore)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Asia Pacific (Sydney)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Asia Pacific (Tokyo)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Canada (Central)	–	–	–
China (Beijing)	–	–	–
China (Ningxia)	–	–	–
Europe (Frankfurt)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Europe (Ireland)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Europe (London)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR

Region	RDS for Oracle 19c	RDS for Oracle 18c	RDS for Oracle 12c
Europe (Milan)	–	–	–
Europe (Paris)	–	–	–
Europe (Spain)	–	–	–
Europe (Stockholm)	19c with the January 2021 or higher RU/RUR	18c with the January 2021 or higher RU/RUR	12.1 and 12.2 with the January 2021 or higher RU/RUR
Europe (Zurich)	–	–	–
Middle East (Bahrain)	–	–	–
Middle East (UAE)	–	–	–
South America (São Paulo)	–	–	–
AWS GovCloud (US-East)	–	–	–
AWS GovCloud (US-West)	–	–	–

RDS Custom with RDS for SQL Server

Following are the supported engine versions and Region availability for RDS Custom with RDS for SQL Server.

Region	RDS for SQL Server 2019
US East (Ohio)	Enterprise, Standard, or Web
US East (N. Virginia)	Enterprise, Standard, or Web
US West (N. California)	–
US West (Oregon)	Enterprise, Standard, or Web
Africa (Cape Town)	–
Asia Pacific (Hong Kong)	–

Region	RDS for SQL Server 2019
Asia Pacific (Hyderabad)	–
Asia Pacific (Jakarta)	–
Asia Pacific (Mumbai)	Enterprise, Standard, or Web
Asia Pacific (Osaka)	–
Asia Pacific (Seoul)	Enterprise, Standard, or Web
Asia Pacific (Singapore)	Enterprise, Standard, or Web
Asia Pacific (Sydney)	Enterprise, Standard, or Web
Asia Pacific (Tokyo)	Enterprise, Standard, or Web
Canada (Central)	Enterprise, Standard, or Web
China (Beijing)	–
China (Ningxia)	–
Europe (Frankfurt)	Enterprise, Standard, or Web
Europe (Ireland)	Enterprise, Standard, or Web
Europe (London)	Enterprise, Standard, or Web
Europe (Milan)	–
Europe (Paris)	–
Europe (Spain)	–
Europe (Stockholm)	Enterprise, Standard, or Web
Europe (Zurich)	–
Middle East (Bahrain)	–
Middle East (UAE)	–
South America (São Paulo)	Enterprise, Standard, or Web
AWS GovCloud (US-East)	–
AWS GovCloud (US-West)	–

Amazon RDS Proxy

Amazon RDS Proxy is a fully managed, highly available database proxy that makes applications more scalable by pooling and sharing established database connections. For more information, see [Using Amazon RDS Proxy \(p. 921\)](#).

RDS Proxy isn't available with RDS for Oracle.

Topics

- [RDS Proxy with RDS for MariaDB \(p. 115\)](#)

- [RDS Proxy with RDS for MySQL \(p. 116\)](#)
- [RDS Proxy with RDS for PostgreSQL \(p. 117\)](#)
- [RDS Proxy with RDS for SQL Server \(p. 119\)](#)

RDS Proxy with RDS for MariaDB

Following are the supported engines and Region availability for RDS Proxy with RDS for MariaDB.

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
US East (Ohio)	–	All versions	All versions	All versions
US East (N. Virginia)	–	All versions	All versions	All versions
US West (N. California)	–	All versions	All versions	All versions
US West (Oregon)	–	All versions	All versions	All versions
Africa (Cape Town)	–	All versions	All versions	All versions
Asia Pacific (Hong Kong)	–	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–
Asia Pacific (Mumbai)	–	All versions	All versions	All versions
Asia Pacific (Osaka)	–	All versions	All versions	All versions
Asia Pacific (Seoul)	–	All versions	All versions	All versions
Asia Pacific (Singapore)	–	All versions	All versions	All versions
Asia Pacific (Sydney)	–	All versions	All versions	All versions
Asia Pacific (Tokyo)	–	All versions	All versions	All versions
Canada (Central)	–	All versions	All versions	All versions
China (Beijing)	–	–	–	–
China (Ningxia)	–	–	–	–
Europe (Frankfurt)	–	All versions	All versions	All versions
Europe (Ireland)	–	All versions	All versions	All versions
Europe (London)	–	All versions	All versions	All versions
Europe (Milan)	–	All versions	All versions	All versions
Europe (Paris)	–	All versions	All versions	All versions
Europe (Spain)	–	–	–	–

Region	RDS for MariaDB 10.6	RDS for MariaDB 10.5	RDS for MariaDB 10.4	RDS for MariaDB 10.3
Europe (Stockholm)	–	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	–	All versions	All versions	All versions
Middle East (UAE)	–	–	–	–
South America (São Paulo)	–	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–

RDS Proxy with RDS for MySQL

Following are the supported engines and Region availability for RDS Proxy with RDS for MySQL.

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
US East (Ohio)	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–
Asia Pacific (Jakarta)	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions
China (Beijing)	–	–	–
China (Ningxia)	–	–	–

Region	RDS for MySQL 8.0	RDS for MySQL 5.7	RDS for MySQL 5.6
Europe (Frankfurt)	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions
Europe (Spain)	–	–	–
Europe (Stockholm)	All versions	All versions	All versions
Europe (Zurich)	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions
Middle East (UAE)	–	–	–
South America (São Paulo)	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–
AWS GovCloud (US-West)	–	–	–

RDS Proxy with RDS for PostgreSQL

Following are the supported engines and Region availability for RDS Proxy with RDS for PostgreSQL.

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
US East (Ohio)	–	All versions	All versions	All versions	All versions
US East (N. Virginia)	–	All versions	All versions	All versions	All versions
US West (N. California)	–	All versions	All versions	All versions	All versions
US West (Oregon)	–	All versions	All versions	All versions	All versions
Africa (Cape Town)	–	All versions	All versions	All versions	All versions
Asia Pacific (Hong Kong)	–	All versions	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–	–

Region	RDS for PostgreSQL 14	RDS for PostgreSQL 13	RDS for PostgreSQL 12	RDS for PostgreSQL 11	RDS for PostgreSQL 10
Asia Pacific (Mumbai)	–	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	–	All versions	All versions	All versions	All versions
Asia Pacific (Seoul)	–	All versions	All versions	All versions	All versions
Asia Pacific (Singapore)	–	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	–	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	–	All versions	All versions	All versions	All versions
Canada (Central)	–	All versions	All versions	All versions	All versions
China (Beijing)	–	–	–	–	–
China (Ningxia)	–	–	–	–	–
Europe (Frankfurt)	–	All versions	All versions	All versions	All versions
Europe (Ireland)	–	All versions	All versions	All versions	All versions
Europe (London)	–	All versions	All versions	All versions	All versions
Europe (Milan)	–	All versions	All versions	All versions	All versions
Europe (Paris)	–	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–	–
Europe (Stockholm)	–	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–	–
Middle East (Bahrain)	–	All versions	All versions	All versions	All versions
Middle East (UAE)	–	–	–	–	–
South America (São Paulo)	–	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–	–

RDS Proxy with RDS for SQL Server

Following are the supported engines and Region availability for RDS Proxy with RDS for SQL Server.

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
US East (Ohio)	All versions	All versions	All versions	All versions
US East (N. Virginia)	All versions	All versions	All versions	All versions
US West (N. California)	All versions	All versions	All versions	All versions
US West (Oregon)	All versions	All versions	All versions	All versions
Africa (Cape Town)	All versions	All versions	All versions	All versions
Asia Pacific (Hong Kong)	All versions	All versions	All versions	All versions
Asia Pacific (Hyderabad)	–	–	–	–
Asia Pacific (Jakarta)	–	–	–	–
Asia Pacific (Mumbai)	All versions	All versions	All versions	All versions
Asia Pacific (Osaka)	All versions	All versions	All versions	All versions
Asia Pacific (Seoul)	All versions	All versions	All versions	All versions
Asia Pacific (Singapore)	All versions	All versions	All versions	All versions
Asia Pacific (Sydney)	All versions	All versions	All versions	All versions
Asia Pacific (Tokyo)	All versions	All versions	All versions	All versions
Canada (Central)	All versions	All versions	All versions	All versions
China (Beijing)	–	–	–	–
China (Ningxia)	–	–	–	–
Europe (Frankfurt)	All versions	All versions	All versions	All versions
Europe (Ireland)	All versions	All versions	All versions	All versions
Europe (London)	All versions	All versions	All versions	All versions
Europe (Milan)	All versions	All versions	All versions	All versions
Europe (Paris)	All versions	All versions	All versions	All versions
Europe (Spain)	–	–	–	–
Europe (Stockholm)	All versions	All versions	All versions	All versions
Europe (Zurich)	–	–	–	–
Middle East (Bahrain)	All versions	All versions	All versions	All versions

Region	RDS for SQL Server 2019	RDS for SQL Server 2017	RDS for SQL Server 2016	RDS for SQL Server 2014
Middle East (UAE)	–	–	–	–
South America (São Paulo)	All versions	All versions	All versions	All versions
AWS GovCloud (US-East)	–	–	–	–
AWS GovCloud (US-West)	–	–	–	–

Engine-native features

Amazon RDS database engines also support many of the most common engine-native features and functionality. These features are different than the Amazon RDS-native features listed on this page. Some engine-native features might have limited support or restricted privileges.

For more information on engine-native features, see:

- [MariaDB feature support on Amazon RDS \(p. 975\)](#)
- [MySQL feature support on Amazon RDS \(p. 1312\)](#)
- [RDS for Oracle features \(p. 1467\)](#)
- [Working with PostgreSQL features supported by Amazon RDS for PostgreSQL \(p. 1905\)](#)
- [Microsoft SQL Server features on Amazon RDS \(p. 1068\)](#)

Multi-AZ deployments for high availability

Multi-AZ deployments can have one standby or two standby DB instances. When the deployment has one standby DB instance, it's called a *Multi-AZ DB instance deployment*. A Multi-AZ DB instance deployment has one standby DB instance that provides failover support, but doesn't serve read traffic. When the deployment has two standby DB instances, it's called a *Multi-AZ DB cluster deployment*. A Multi-AZ DB cluster deployment has standby DB instances that provide failover support and can also serve read traffic.

You can use the AWS Management Console to determine whether a Multi-AZ deployment is a Multi-AZ DB instance deployment or a Multi-AZ DB cluster deployment. In the navigation pane, choose **Databases**, and then choose a **DB identifier**.

- A Multi-AZ DB instance deployment has the following characteristics:
 - There is only one row for the DB instance.
 - The value of **Role** is **Instance or Primary**.
 - The value of **Multi-AZ** is **Yes**.
- A Multi-AZ DB cluster deployment has the following characteristics:
 - There is a cluster-level row with three DB instance rows under it.
 - For the cluster-level row, the value of **Role** is **Multi-AZ DB cluster**.
 - For each instance-level row, the value of **Role** is **Writer instance** or **Reader instance**.
 - For each instance-level row, the value of **Multi-AZ** is **3 Zones**.

Topics

- [Multi-AZ DB instance deployments \(p. 122\)](#)
- [Multi-AZ DB cluster deployments \(p. 127\)](#)

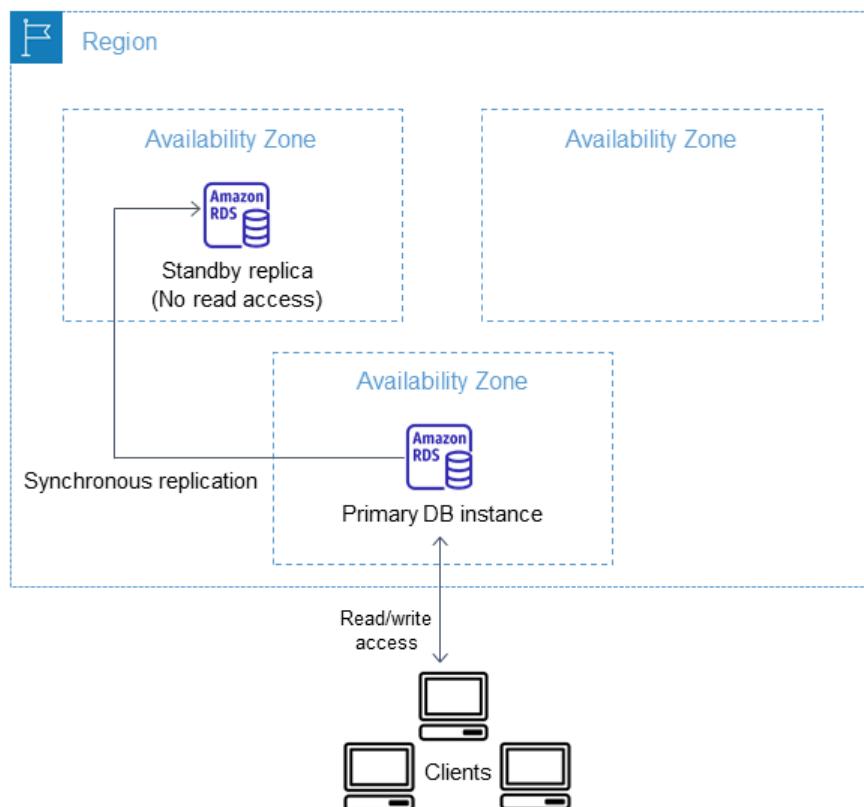
Multi-AZ DB instance deployments

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments with a single standby DB instance. This type of deployment is called a *Multi-AZ DB instance deployment*. Amazon RDS uses several different technologies to provide this failover support. Multi-AZ deployments for MariaDB, MySQL, Oracle, and PostgreSQL DB instances use the Amazon failover technology. Microsoft SQL Server DB instances use SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). For information on SQL Server version support for Multi-AZ, see [Multi-AZ deployments for Amazon RDS for Microsoft SQL Server \(p. 1129\)](#).

In a Multi-AZ DB instance deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different Availability Zone. The primary DB instance is synchronously replicated across Availability Zones to a standby replica to provide data redundancy and minimize latency spikes during system backups. Running a DB instance with high availability can enhance availability during planned system maintenance. It can also help protect your databases against DB instance failure and Availability Zone disruption. For more information on Availability Zones, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

Note

The high availability option isn't a scaling solution for read-only scenarios. You can't use a standby replica to serve read traffic. To serve read-only traffic, use a Multi-AZ DB cluster or a read replica instead. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#). For more information about read replicas, see [Working with read replicas \(p. 370\)](#).



Using the RDS console, you can create a Multi-AZ DB instance deployment by simply specifying Multi-AZ when creating a DB instance. You can use the console to convert existing DB instances to Multi-AZ DB instance deployments by modifying the DB instance and specifying the Multi-AZ option. You can also specify a Multi-AZ DB instance deployment with the AWS CLI or Amazon RDS API. Use the [create-](#)

[db-instance](#) or [modify-db-instance](#) CLI command, or the [CreateDBInstance](#) or [ModifyDBInstance](#) API operation.

The RDS console shows the Availability Zone of the standby replica (called the secondary AZ). You can also use the [describe-db-instances](#) CLI command or the [DescribeDBInstances](#) API operation to find the secondary AZ.

DB instances using Multi-AZ DB instance deployments can have increased write and commit latency compared to a Single-AZ deployment. This can happen because of the synchronous data replication that occurs. You might have a change in latency if your deployment fails over to the standby replica, although AWS is engineered with low-latency network connectivity between Availability Zones. For production workloads, we recommend that you use Provisioned IOPS (input/output operations per second) for fast, consistent performance. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).

Modifying a DB instance to be a Multi-AZ DB instance deployment

If you have a DB instance in a Single-AZ deployment and modify it to a Multi-AZ DB instance deployment (for engines other than Amazon Aurora), Amazon RDS performs several actions:

1. Takes a snapshot of the primary DB instance's Amazon Elastic Block Store (EBS) volumes.
2. Creates new volumes for the standby replica from the snapshot. These volumes initialize in the background, and maximum volume performance is achieved after the data is fully initialized.
3. Turns on synchronous block-level replication between the volumes of the primary and standby replicas.

Important

Using a snapshot to create the standby instance avoids downtime when you convert from Single-AZ to Multi-AZ, but you can experience a performance impact during and after converting to Multi-AZ. This impact can be significant for workloads that are sensitive to write latency.

While this capability lets large volumes be restored from snapshots quickly, it can cause a significant increase in the latency of I/O operations because of the synchronous replication. This latency can impact your database performance. We highly recommend as a best practice not to perform Multi-AZ conversion on a production DB instance.

To avoid the performance impact on the DB instance currently serving the sensitive workload, create a read replica and enable backups on the read replica. Convert the read replica to Multi-AZ, and run queries that load the data into the read replica's volumes (on both AZs). Then promote the read replica to be the primary DB instance. For more information, see [Working with read replicas \(p. 370\)](#).

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#). After the modification is complete, Amazon RDS triggers an event (RDS-EVENT-0025) that indicates the process is complete. You can monitor Amazon RDS events. For more information about events, see [Working with Amazon RDS event notification \(p. 650\)](#).

Failover process for Amazon RDS

If a planned or unplanned outage of your DB instance results from an infrastructure defect, Amazon RDS automatically switches to a standby replica in another Availability Zone if you have turned on Multi-AZ. The time that it takes for the failover to complete depends on the database activity and other conditions at the time the primary DB instance became unavailable. Failover times are typically 60–120 seconds. However, large transactions or a lengthy recovery process can increase failover time. When the failover is complete, it can take additional time for the RDS console to reflect the new Availability Zone.

Note

You can force a failover manually when you reboot a DB instance. For more information, see [Rebooting a DB instance \(p. 366\)](#).

Amazon RDS handles failovers automatically so you can resume database operations as quickly as possible without administrative intervention. The primary DB instance switches over automatically to the standby replica if any of the conditions described in the following table occurs. You can view these failover reasons in the event log.

Failover reason	Description
The operating system underlying the RDS database instance is being patched in an offline operation.	<p>A failover was triggered during the maintenance window for an OS patch or a security update.</p> <p>For more information, see Maintaining a DB instance (p. 350).</p>
The primary host of the RDS Multi-AZ instance is unhealthy.	The Multi-AZ DB instance deployment detected an impaired primary DB instance and failed over.
The primary host of the RDS Multi-AZ instance is unreachable due to loss of network connectivity.	RDS monitoring detected a network reachability failure to the primary DB instance and triggered a failover.
The RDS instance was modified by customer.	<p>An RDS DB instance modification triggered a failover.</p> <p>For more information, see Modifying an Amazon RDS DB instance (p. 327).</p>
The RDS Multi-AZ primary instance is busy and unresponsive.	<p>The primary DB instance is unresponsive. We recommend that you do the following:</p> <ul style="list-style-type: none"> • Examine the event and CloudWatch logs for excessive CPU, memory, or swap space usage. For more information, see Working with Amazon RDS event notification (p. 650) and Creating a rule that triggers on an Amazon RDS event (p. 664). • Evaluate your workload to determine whether you're using the appropriate DB instance class. For more information, see DB instance classes (p. 10). • Use Enhanced Monitoring for real-time operating system metrics. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600). • Use Performance Insights to help analyze any issues that affect your DB instance's performance. For more information, see Monitoring DB load with Performance Insights on Amazon RDS (p. 543). <p>For more information on these recommendations, see Overview of monitoring metrics in Amazon RDS (p. 511) and Best practices for Amazon RDS (p. 216).</p>

Failover reason	Description
The storage volume underlying the primary host of the RDS Multi-AZ instance experienced a failure.	The Multi-AZ DB instance deployment detected a storage issue on the primary DB instance and failed over.
The user requested a failover of the DB instance.	<p>You rebooted the DB instance and chose Reboot with failover.</p> <p>For more information, see Rebooting a DB instance (p. 366).</p>

To determine if your Multi-AZ DB instance has failed over, you can do the following:

- Set up DB event subscriptions to notify you by email or SMS that a failover has been initiated. For more information about events, see [Working with Amazon RDS event notification \(p. 650\)](#).
- View your DB events by using the RDS console or API operations.
- View the current state of your Multi-AZ DB instance deployment by using the RDS console or API operations.

For information on how you can respond to failovers, reduce recovery time, and other best practices for Amazon RDS, see [Best practices for Amazon RDS \(p. 216\)](#).

Setting the JVM TTL for DNS name lookups

The failover mechanism automatically changes the Domain Name System (DNS) record of the DB instance to point to the standby DB instance. As a result, you need to re-establish any existing connections to your DB instance. In a Java virtual machine (JVM) environment, due to how the Java DNS caching mechanism works, you might need to reconfigure JVM settings.

The JVM caches DNS name lookups. When the JVM resolves a host name to an IP address, it caches the IP address for a specified period of time, known as the *time-to-live* (TTL).

Because AWS resources use DNS name entries that occasionally change, we recommend that you configure your JVM with a TTL value of no more than 60 seconds. Doing this makes sure that when a resource's IP address changes, your application can receive and use the resource's new IP address by querying the DNS.

On some Java configurations, the JVM default TTL is set so that it never refreshes DNS entries until the JVM is restarted. Thus, if the IP address for an AWS resource changes while your application is still running, it can't use that resource until you manually restart the JVM and the cached IP information is refreshed. In this case, it's crucial to set the JVM's TTL so that it periodically refreshes its cached IP information.

Note

The default TTL can vary according to the version of your JVM and whether a security manager is installed. Many JVMs provide a default TTL less than 60 seconds. If you're using such a JVM and not using a security manager, you can ignore the rest of this topic. For more information on security managers in Oracle, see [The security manager](#) in the Oracle documentation.

To modify the JVM's TTL, set the `networkaddress.cache.ttl` property value. Use one of the following methods, depending on your needs:

- To set the property value globally for all applications that use the JVM, set `networkaddress.cache.ttl` in the `$JAVA_HOME/jre/lib/security/java.security` file.

```
networkaddress.cache.ttl=60
```

- To set the property locally for your application only, set `networkaddress.cache.ttl` in your application's initialization code before any network connections are established.

```
java.security.Security.setProperty("networkaddress.cache.ttl" , "60");
```

Multi-AZ DB cluster deployments

A *Multi-AZ DB cluster deployment* is a high availability deployment mode of Amazon RDS with two readable standby DB instances. A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones in the same AWS Region. Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower write latency when compared to Multi-AZ DB instance deployments.

Topics

- [Region and version availability \(p. 127\)](#)
- [Overview of Multi-AZ DB clusters \(p. 127\)](#)
- [Creating and managing a Multi-AZ DB cluster \(p. 128\)](#)
- [Managing connections for Multi-AZ DB clusters \(p. 129\)](#)
- [Managing a Multi-AZ DB cluster with the AWS Management Console \(p. 131\)](#)
- [Working with parameter groups for Multi-AZ DB clusters \(p. 133\)](#)
- [Replica lag and Multi-AZ DB clusters \(p. 133\)](#)
- [Failover process for Multi-AZ DB clusters \(p. 134\)](#)
- [Limitations for Multi-AZ DB clusters \(p. 136\)](#)

Important

Multi-AZ DB clusters aren't the same as Aurora DB clusters. For information about Aurora DB clusters, see the [Amazon Aurora User Guide](#).

Region and version availability

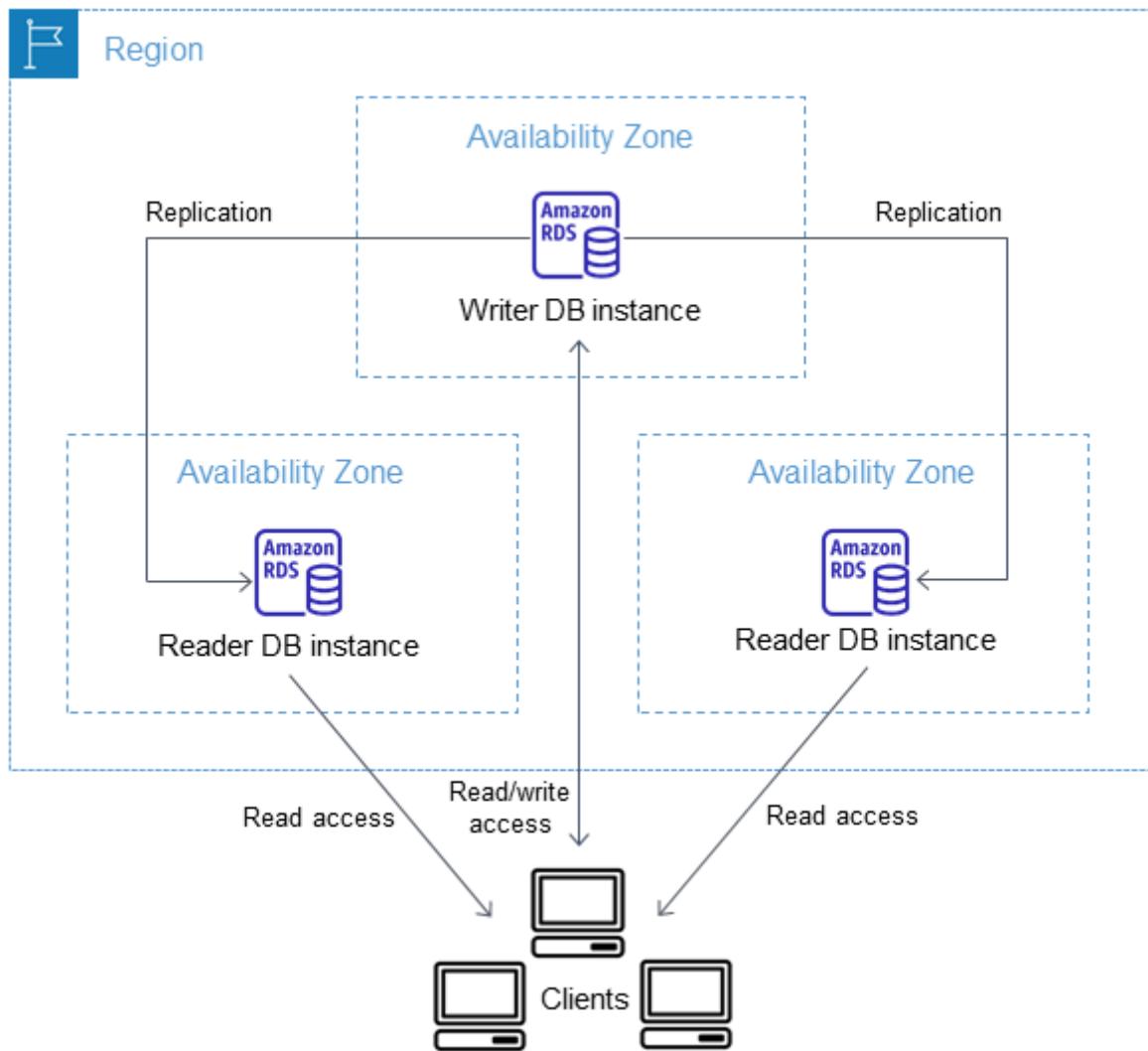
Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of Amazon RDS with Multi-AZ DB clusters, see [Multi-AZ DB clusters \(p. 107\)](#).

Overview of Multi-AZ DB clusters

With a Multi-AZ DB cluster, Amazon RDS replicates data from the writer DB instance to both of the reader DB instances using the DB engine's native replication capabilities. When a change is made on the writer DB instance, it's sent to each reader DB instance. Acknowledgment from at least one reader DB instance is required for a change to be committed.

Reader DB instances act as automatic failover targets and also serve read traffic to increase application read throughput. If an outage occurs on your writer DB instance, RDS manages failover to one of the reader DB instances. RDS does this based on which reader DB instance has the most recent change record.

The following diagram shows a Multi-AZ DB cluster.



Multi-AZ DB clusters typically have lower write latency when compared to Multi-AZ DB instance deployments. They also allow read-only workloads to run on reader DB instances. The RDS console shows the Availability Zone of the writer DB instance and the Availability Zones of the reader DB instances. You can also use the [describe-db-clusters](#) CLI command or the [DescribeDBClusters](#) API operation to find this information.

Creating and managing a Multi-AZ DB cluster

You can create a Multi-AZ DB cluster directly or by restoring from a snapshot. For instructions, see these topics:

- [Creating a Multi-AZ DB cluster \(p. 252\)](#)
- [Restoring from a snapshot to a Multi-AZ DB cluster \(p. 456\)](#)

You can modify, reboot, or delete a Multi-AZ DB by following the instructions in these topics:

- [Modifying a Multi-AZ DB cluster \(p. 341\)](#)
- [Rebooting Multi-AZ DB clusters and reader DB instances \(p. 368\)](#)

- [Deleting a Multi-AZ DB cluster \(p. 424\)](#)

You can create a snapshot of a Multi-AZ DB cluster by following the instructions in [Creating a Multi-AZ DB cluster snapshot \(p. 450\)](#).

You can restore a Multi-AZ DB cluster to a point in time by following the instructions in [Restoring a Multi-AZ DB cluster to a specified time \(p. 502\)](#).

Managing connections for Multi-AZ DB clusters

A Multi-AZ DB cluster has three DB instances instead of a single DB instance. Each connection is handled by a specific DB instance. When you connect to a Multi-AZ DB cluster, the host name and port that you specify point to a fully qualified domain name called an *endpoint*. The Multi-AZ DB cluster uses the endpoint mechanism to abstract these connections. Thus, you don't have to hardcode all the host names or write your own logic for rerouting connections when some DB instances aren't available.

The writer endpoint connects to the writer DB instance of the DB cluster, which supports both read and write operations. The reader endpoint connects to either of the two reader DB instances, which support only read operations.

Using endpoints, you can map each connection to the appropriate DB instance or group of DB instances based on your use case. For example, to perform DDL and DML statements, you can connect to whichever DB instance is the writer DB instance. To perform queries, you can connect to the reader endpoint, with the Multi-AZ DB cluster automatically managing connections among the reader DB instances. For diagnosis or tuning, you can connect to a specific DB instance endpoint to examine details about a specific DB instance.

For information about connecting to a DB instance, see [Connecting to an Amazon RDS DB instance \(p. 267\)](#).

Topics

- [Types of Multi-AZ DB cluster endpoints \(p. 129\)](#)
- [Viewing the endpoints for a Multi-AZ DB cluster \(p. 130\)](#)
- [Using the cluster endpoint \(p. 130\)](#)
- [Using the reader endpoint \(p. 131\)](#)
- [Using the instance endpoints \(p. 131\)](#)
- [How Multi-AZ DB endpoints work with high availability \(p. 131\)](#)

Types of Multi-AZ DB cluster endpoints

An endpoint is represented by a unique identifier that contains a host address. The following types of endpoints are available from a Multi-AZ DB cluster:

Cluster endpoint

A *cluster endpoint* (or *writer endpoint*) for a Multi-AZ DB cluster connects to the current writer DB instance for that DB cluster. This endpoint is the only one that can perform write operations such as DDL and DML statements. This endpoint can also perform read operations.

Each Multi-AZ DB cluster has one cluster endpoint and one writer DB instance.

You use the cluster endpoint for all write operations on the DB cluster, including inserts, updates, deletes, and DDL changes. You can also use the cluster endpoint for read operations, such as queries.

If the current writer DB instance of a DB cluster fails, the Multi-AZ DB cluster automatically fails over to a new writer DB instance. During a failover, the DB cluster continues to serve connection requests to the cluster endpoint from the new writer DB instance, with minimal interruption of service.

The following example illustrates a cluster endpoint for a Multi-AZ DB cluster.

`mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com`

Reader endpoint

A *reader endpoint* for a Multi-AZ DB cluster provides support for read-only connections to the DB cluster. Use the reader endpoint for read operations, such as SELECT queries. By processing those statements on the reader DB instances, this endpoint reduces the overhead on the writer DB instance. It also helps the cluster to scale the capacity to handle simultaneous SELECT queries. Each Multi-AZ DB cluster has one reader endpoint.

The reader endpoint sends each connection request to one of the reader DB instances. When you use the reader endpoint for a session, you can only perform read-only statements such as SELECT in that session.

The following example illustrates a reader endpoint for a Multi-AZ DB cluster. The read-only intent of a reader endpoint is denoted by the `-ro` within the cluster endpoint name.

`mydbcluster.cluster-ro-123456789012.us-east-1.rds.amazonaws.com`

Instance endpoint

An *instance endpoint* connects to a specific DB instance within a Multi-AZ DB cluster. Each DB instance in a DB cluster has its own unique instance endpoint. So there is one instance endpoint for the current writer DB instance of the DB cluster, and there is one instance endpoint for each of the reader DB instances in the DB cluster.

The instance endpoint provides direct control over connections to the DB cluster. This control can help you address scenarios where using the cluster endpoint or reader endpoint might not be appropriate. For example, your client application might require more fine-grained load balancing based on workload type. In this case, you can configure multiple clients to connect to different reader DB instances in a DB cluster to distribute read workloads.

The following example illustrates an instance endpoint for a DB instance in a Multi-AZ DB cluster.

`mydbinstance.123456789012.us-east-1.rds.amazonaws.com`

Viewing the endpoints for a Multi-AZ DB cluster

In the AWS Management Console, you see the cluster endpoint and the reader endpoint on the details page for each Multi-AZ DB cluster. You see the instance endpoint in the details page for each DB instance.

With the AWS CLI, you see the writer and reader endpoints in the output of the `describe-db-clusters` command. For example, the following command shows the endpoint attributes for all clusters in your current AWS Region.

```
aws rds describe-db-cluster-endpoints
```

With the Amazon RDS API, you retrieve the endpoints by calling the `DescribeDBClusterEndpoints` action. The output also shows Amazon Aurora DB cluster endpoints, if any exist.

Using the cluster endpoint

Each Multi-AZ DB cluster has a single built-in cluster endpoint, whose name and other attributes are managed by Amazon RDS. You can't create, delete, or modify this kind of endpoint.

You use the cluster endpoint when you administer your DB cluster, perform extract, transform, load (ETL) operations, or develop and test applications. The cluster endpoint connects to the writer DB instance of

the cluster. The writer DB instance is the only DB instance where you can create tables and indexes, run INSERT statements, and perform other DDL and DML operations.

The physical IP address pointed to by the cluster endpoint changes when the failover mechanism promotes a new DB instance to be the writer DB instance for the cluster. If you use any form of connection pooling or other multiplexing, be prepared to flush or reduce the time-to-live for any cached DNS information. Doing so ensures that you don't try to establish a read/write connection to a DB instance that became unavailable or is now read-only after a failover.

Using the reader endpoint

You use the reader endpoint for read-only connections to your Multi-AZ DB cluster. This endpoint helps your DB cluster handle a query-intensive workload. The reader endpoint is the endpoint that you supply to applications that do reporting or other read-only operations on the cluster. The reader endpoint sends connections to available reader DB instances in a Multi-AZ DB cluster.

Each Multi-AZ cluster has a single built-in reader endpoint, whose name and other attributes are managed by Amazon RDS. You can't create, delete, or modify this kind of endpoint.

Using the instance endpoints

Each DB instance in a Multi-AZ DB cluster has its own built-in instance endpoint, whose name and other attributes are managed by Amazon RDS. You can't create, delete, or modify this kind of endpoint. With a Multi-AZ DB cluster, you typically use the writer and reader endpoints more often than the instance endpoints.

In day-to-day operations, the main way that you use instance endpoints is to diagnose capacity or performance issues that affect one specific DB instance in a Multi-AZ DB cluster. While connected to a specific DB instance, you can examine its status variables, metrics, and so on. Doing this can help you determine what's happening for that DB instance that's different from what's happening for other DB instances in the cluster.

How Multi-AZ DB endpoints work with high availability

For Multi-AZ DB clusters where high availability is important, use the writer endpoint for read/write or general-purpose connections and the reader endpoint for read-only connections. The writer and reader endpoints manage DB instance failover better than instance endpoints do. Unlike the instance endpoints, the writer and reader endpoints automatically change which DB instance they connect to if a DB instance in your cluster becomes unavailable.

If the writer DB instance of a DB cluster fails, Amazon RDS automatically fails over to a new writer DB instance. It does so by promoting a reader DB instance to a new writer DB instance. If a failover occurs, you can use the writer endpoint to reconnect to the newly promoted writer DB instance. Or you can use the reader endpoint to reconnect to one of the reader DB instances in the DB cluster. During a failover, the reader endpoint might direct connections to the new writer DB instance of a DB cluster for a short time after a reader DB instance is promoted to the new writer DB instance. If you design your own application logic to manage instance endpoint connections, you can manually or programmatically discover the resulting set of available DB instances in the DB cluster.

Managing a Multi-AZ DB cluster with the AWS Management Console

You can manage a Multi-AZ DB cluster with the console.

To manage a Multi-AZ DB cluster with the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**, and then choose the Multi-AZ DB cluster that you want to manage.

The following image shows a Multi-AZ DB cluster in the console.

DB identifier	Role	Engine	Region & AZ	Size
my-multi-az-cluster	Multi-AZ DB cluster	PostgreSQL	us-west-2	3 instances
my-multi-az-cluster-instance-1	Writer instance	PostgreSQL	us-west-2a	db.m6gd.xlarge
my-multi-az-cluster-instance-2	Reader instance	PostgreSQL	us-west-2c	db.m6gd.xlarge
my-multi-az-cluster-instance-3	Reader instance	PostgreSQL	us-west-2b	db.m6gd.xlarge

The available actions in the **Actions** menu depend on whether the Multi-AZ DB cluster is selected or a DB instance in the cluster is selected.

Choose the Multi-AZ DB cluster to view the cluster details and perform actions at the cluster level.

Choose a DB instance in a Multi-AZ DB cluster to view the DB instance details and perform actions at the DB instance level.

Working with parameter groups for Multi-AZ DB clusters

In a Multi-AZ DB cluster, a *DB cluster parameter group* acts as a container for engine configuration values that are applied to every DB instance in the Multi-AZ DB cluster.

In a Multi-AZ DB cluster, a *DB parameter group* is set to the default DB parameter group for the DB engine and DB engine version. The settings in the DB cluster parameter group are used for all of the DB instances in the cluster.

For information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

Replica lag and Multi-AZ DB clusters

Replica lag is the difference in time between the latest transaction on the writer DB instance and the latest applied transaction on a reader DB instance. The Amazon CloudWatch metric `ReplicaLag` represents this time difference. For more information about CloudWatch metrics, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).

Although Multi-AZ DB clusters allow for high write performance, replica lag can still occur due to the nature of engine-based replication. Because any failover must first resolve the replica lag before it promotes a new writer DB instance, monitoring and managing this replica lag is a consideration.

For RDS for MySQL Multi-AZ DB clusters, failover time depends on replica lag of both remaining reader DB instances. Both the reader DB instances must apply unapplied transactions before one of them is promoted to the new writer DB instance.

For RDS for PostgreSQL Multi-AZ DB clusters, failover time depends on the lowest replica lag of the two remaining reader DB instances. The reader DB instance with the lowest replica lag must apply unapplied transactions before it is promoted to the new writer DB instance.

For a tutorial that shows you how to create a CloudWatch alarm when replica lag exceeds a set amount of time, see [Tutorial: Creating an Amazon CloudWatch alarm for Multi-AZ DB cluster replica lag \(p. 536\)](#).

Common causes of replica lag

In general, replica lag occurs when the write workload is too high for the reader DB instances to apply the transactions efficiently. Various workloads can incur temporary or continuous replica lag. Some examples of common causes are the following:

- High write concurrency or heavy batch updating on the writer DB instance, causing the apply process on the reader DB instances to fall behind.
- Heavy read workload that is using resources on one or more reader DB instances. Running slow or large queries can affect the apply process and can cause replica lag.
- Transactions that modify large amounts of data or DDL statements can sometimes cause a temporary increase in replica lag because the database must preserve commit order.

Mitigating replica lag

For Multi-AZ DB clusters for RDS for MySQL and RDS for PostgreSQL, you can mitigate replica lag by reducing the load on your writer DB instance. You can also use flow control to reduce replica lag. *Flow control* works by throttling writes on the writer DB instance, which ensures that replica lag doesn't continue to grow unbounded. Write throttling is accomplished by adding a delay into the end of a transaction, which decreases the write throughput on the writer DB instance. Although flow control doesn't guarantee lag elimination, it can help reduce overall lag in many workloads. The following sections provide information about using flow control with RDS for MySQL and RDS for PostgreSQL.

Mitigating replica lag with flow control for RDS for MySQL

When you are using RDS for MySQL Multi-AZ DB clusters, flow control is turned on by default using the dynamic parameter `rpl_semi_sync_master_target_apply_lag`. This parameter specifies the upper limit that you want for replica lag. As replica lag approaches this configured limit, flow control throttles the write transactions on the writer DB Instance to try to contain the replica lag below the specified value. In some cases, replica lag can exceed the specified limit. By default, this parameter is set to 120 seconds. To turn off flow control, set this parameter to its maximum value of 86400 seconds (one day).

To view the current delay injected by flow control, show the parameter `Rpl_semi_sync_master_flow_control_current_delay` by running the following query.

```
SHOW GLOBAL STATUS like '%flow_control%';
```

Your output looks similar to the following.

Variable_name	Value
Rpl_semi_sync_master_flow_control_current_delay	2010

1 row in set (0.00 sec)

Note

The delay is shown in microseconds.

When you have Performance Insights turned on for an RDS for MySQL Multi-AZ DB cluster, you can monitor the wait event corresponding to a SQL statement indicating that the queries were delayed by a flow control. When a delay was introduced by a flow control, you can view the wait event / `wait/synch/cond/semisync/semi_sync_flow_control_delay_cond` corresponding to the SQL statement on the Performance Insights dashboard. To view these metrics, make sure that the Performance Schema is turned on. For information about Performance Insights, see [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#).

Mitigating replica lag with flow control for RDS for PostgreSQL

When you are using RDS for PostgreSQL Multi-AZ DB clusters, flow control is deployed as an extension. It turns on a background worker for all DB instances in the DB cluster. By default, the background workers on the reader DB instances communicate the current replica lag with the background worker on the writer DB instance. If the lag exceeds two minutes on any reader DB instance, the background worker on the writer DB instance adds a delay at the end of a transaction. To control the lag threshold, use the parameter `flow_control.target_standby_apply_lag`.

When a flow control throttles a PostgreSQL process, the Extension wait event in `pg_stat_activity` and Performance Insights indicates that. The function `get_flow_control_stats` displays details about how much delay is currently being added.

Flow control can benefit most online transaction processing (OLTP) workloads that have short but highly concurrent transactions. If the lag is caused by long-running transactions, such as batch operations, flow control doesn't provide as strong a benefit.

You can turn off flow control by removing the extension from the `preload_shared_libraries` and rebooting your DB instance.

Failover process for Multi-AZ DB clusters

If there is a planned or unplanned outage of your writer DB instance in a Multi-AZ DB cluster, Amazon RDS automatically fails over to a reader DB instance in different Availability Zone. The time it takes for

the failover to complete depends on the database activity and other conditions when the writer DB instance became unavailable. Failover times are typically under 35 seconds. Failover completes when both reader DB instances have applied outstanding transactions from the failed writer. When the failover is complete, it can take additional time for the RDS console to reflect the new Availability Zone.

Topics

- [Automatic failovers \(p. 135\)](#)
- [Manually failing over a Multi-AZ DB cluster \(p. 135\)](#)
- [Determining whether a Multi-AZ DB cluster has failed over \(p. 135\)](#)
- [Setting the JVM TTL for DNS name lookups \(p. 136\)](#)

Automatic failovers

Amazon RDS handles failovers automatically so you can resume database operations as quickly as possible without administrative intervention. To fail over, the writer DB instance switches automatically to a reader DB instance.

Manually failing over a Multi-AZ DB cluster

You can fail over a Multi-AZ DB cluster manually using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To fail over a Multi-AZ DB cluster manually

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the Multi-AZ DB cluster that you want to fail over.
4. For **Actions**, choose **Failover**.

The **Failover DB Cluster** page appears.

5. Choose **Failover** to confirm the manual failover.

AWS CLI

To fail over a Multi-AZ DB cluster manually, use the AWS CLI command [failover-db-cluster](#).

Example

```
aws rds failover-db-cluster --db-cluster-identifier mymultiazdbcluster
```

RDS API

To fail over a Multi-AZ DB cluster manually, call the Amazon RDS API [FailoverDBCluster](#) and specify the `DBClusterIdentifier`.

Determining whether a Multi-AZ DB cluster has failed over

To determine if your Multi-AZ DB cluster has failed over, you can do the following:

- Set up DB event subscriptions to notify you by email or SMS that a failover has been initiated. For more information about events, see [Working with Amazon RDS event notification \(p. 650\)](#).

- View your DB events by using the Amazon RDS console or API operations.
- View the current state of your Multi-AZ DB cluster by using the Amazon RDS console, the AWS CLI, and the RDS API.

For information on how you can respond to failovers, reduce recovery time, and other best practices for Amazon RDS, see [Best practices for Amazon RDS \(p. 216\)](#).

Setting the JVM TTL for DNS name lookups

The failover mechanism automatically changes the Domain Name System (DNS) record of the DB instance to point to the reader DB instance. As a result, you need to re-establish any existing connections to your DB instance. In a Java virtual machine (JVM) environment, due to how the Java DNS caching mechanism works, you might need to reconfigure JVM settings.

The JVM caches DNS name lookups. When the JVM resolves a host name to an IP address, it caches the IP address for a specified period of time, known as the *time-to-live* (TTL).

Because AWS resources use DNS name entries that occasionally change, we recommend that you configure your JVM with a TTL value of no more than 60 seconds. Doing this makes sure that when a resource's IP address changes, your application can receive and use the resource's new IP address by requerying the DNS.

On some Java configurations, the JVM default TTL is set so that it never refreshes DNS entries until the JVM is restarted. Thus, if the IP address for an AWS resource changes while your application is still running, it can't use that resource until you manually restart the JVM and the cached IP information is refreshed. In this case, it's crucial to set the JVM's TTL so that it periodically refreshes its cached IP information.

Note

The default TTL can vary according to the version of your JVM and whether a security manager is installed. Many JVMs provide a default TTL less than 60 seconds. If you're using such a JVM and not using a security manager, you can ignore the rest of this topic. For more information on security managers in Oracle, see [The security manager](#) in the Oracle documentation.

To modify the JVM's TTL, set the `networkaddress.cache.ttl` property value. Use one of the following methods, depending on your needs:

- To set the property value globally for all applications that use the JVM, set `networkaddress.cache.ttl` in the `$JAVA_HOME/jre/lib/security/java.security` file.

```
networkaddress.cache.ttl=60
```

- To set the property locally for your application only, set `networkaddress.cache.ttl` in your application's initialization code before any network connections are established.

```
java.security.Security.setProperty("networkaddress.cache.ttl" , "60");
```

Limitations for Multi-AZ DB clusters

The following limitations apply to Multi-AZ DB clusters:

- Multi-AZ DB clusters only support Provisioned IOPS storage.

- You can't change a single-AZ DB instance deployment or Multi-AZ DB instance deployment into a Multi-AZ DB cluster. As an alternative, you can restore a snapshot of a single-AZ DB instance deployment or Multi-AZ DB instance deployment to a Multi-AZ DB cluster.
- You can't restore a Multi-AZ DB cluster snapshot to a Multi-AZ DB instance deployment or single-AZ deployment.
- Multi-AZ DB clusters don't support modifications at the DB instance level because all modifications are done at the DB cluster level.
- Multi-AZ DB clusters don't support the following features:
 - Amazon RDS Proxy
 - Support for IPv6 connections (dual-stack mode)
 - Exporting Multi-AZ DB cluster snapshot data to an Amazon S3 bucket
 - IAM DB authentication
 - Kerberos authentication
 - Modifying the port

As an alternative, you can restore a Multi-AZ DB cluster to a point in time and specify a different port.

- Option groups
- Read replicas
- Reserved DB instances
- Restoring a Multi-AZ DB cluster snapshot from an Amazon S3 bucket
- Storage autoscaling by setting the maximum allocated storage

As an alternative, you can scale storage manually.

- Stopping and starting the DB cluster
- Copying a snapshot of a Multi-AZ DB cluster
- Encrypting an unencrypted Multi-AZ DB cluster
- RDS for MySQL Multi-AZ DB clusters don't support replication to an external target database.
- RDS for MySQL Multi-AZ DB clusters support only the following system stored procedures:
 - `mysql.rds_rotate_general_log`
 - `mysql.rds_rotate_slow_log`
 - `mysql.rds_show_configuration`

RDS for MySQL Multi-AZ DB clusters don't support other system stored procedures. For information about these procedures, see [MySQL on Amazon RDS SQL reference \(p. 1439\)](#).

- RDS for PostgreSQL Multi-AZ DB clusters don't support the following PostgreSQL extensions: `aws_s3`, `pg_transport`, and `pglogical`.
- RDS for PostgreSQL Multi-AZ DB clusters don't support using a custom DNS server for outbound network access.
- RDS for PostgreSQL Multi-AZ DB clusters don't support logical replication.

DB instance billing for Amazon RDS

Amazon RDS instances are billed based on the following components:

- DB instance hours (per hour) – Based on the DB instance class of the DB instance (for example, db.t2.small or db.m4.large). Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. RDS usage is billed in 1-second increments, with a minimum of 10 minutes. For more information, see [DB instance classes \(p. 10\)](#).
- Storage (per GiB per month) – Storage capacity that you have provisioned to your DB instance. If you scale your provisioned storage capacity within the month, your bill is prorated. For more information, see [Amazon RDS DB instance storage \(p. 64\)](#).
- I/O requests (per 1 million requests per month) – Total number of storage I/O requests that you have made in a billing cycle, for Amazon RDS magnetic storage only.
- Provisioned IOPS (per IOPS per month) – Provisioned IOPS rate, regardless of IOPS consumed, for Amazon RDS Provisioned IOPS (SSD) and General Purpose (SSD) gp3 storage. Provisioned storage for EBS volumes are billed in 1-second increments, with a minimum of 10 minutes.
- Backup storage (per GiB per month) – *Backup storage* is the storage that is associated with automated database backups and any active database snapshots that you have taken. Increasing your backup retention period or taking additional database snapshots increases the backup storage consumed by your database. Per second billing doesn't apply to backup storage (metered in GB-month).

For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

- Data transfer (per GB) – Data transfer in and out of your DB instance from or to the internet and other AWS Regions.

Amazon RDS provides the following purchasing options to enable you to optimize your costs based on your needs:

- **On-Demand instances** – Pay by the hour for the DB instance hours that you use. Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. RDS usage is now billed in 1-second increments, with a minimum of 10 minutes.
- **Reserved instances** – Reserve a DB instance for a one-year or three-year term and get a significant discount compared to the on-demand DB instance pricing. With Reserved Instance usage, you can launch, delete, start, or stop multiple instances within an hour and get the Reserved Instance benefit for all of the instances.

For Amazon RDS pricing information, see the [Amazon RDS pricing page](#).

Topics

- [On-Demand DB instances for Amazon RDS \(p. 139\)](#)
- [Reserved DB instances for Amazon RDS \(p. 140\)](#)

On-Demand DB instances for Amazon RDS

Amazon RDS on-demand DB instances are billed based on the class of the DB instance (for example, db.t2.small or db.m4.large). For Amazon RDS pricing information, see the [Amazon RDS product page](#).

Billing starts for a DB instance as soon as the DB instance is available. Pricing is listed on a per-hour basis, but bills are calculated down to the second and show times in decimal form. Amazon RDS usage is billed in one-second increments, with a minimum of 10 minutes. In the case of billable configuration change, such as scaling compute or storage capacity, you're charged a 10-minute minimum. Billing continues until the DB instance terminates, which occurs when you delete the DB instance or if the DB instance fails.

If you no longer want to be charged for your DB instance, you must stop or delete it to avoid being billed for additional DB instance hours. For more information about the DB instance states for which you are billed, see [Viewing Amazon RDS DB instance status \(p. 516\)](#).

Stopped DB instances

While your DB instance is stopped, you're charged for provisioned storage, including Provisioned IOPS. You are also charged for backup storage, including storage for manual snapshots and automated backups within your specified retention window. You aren't charged for DB instance hours.

Multi-AZ DB instances

If you specify that your DB instance should be a Multi-AZ deployment, you're billed according to the Multi-AZ pricing posted on the Amazon RDS pricing page.

Reserved DB instances for Amazon RDS

Using reserved DB instances, you can reserve a DB instance for a one- or three-year term. Reserved DB instances provide you with a significant discount compared to on-demand DB instance pricing. Reserved DB instances are not physical instances, but rather a billing discount applied to the use of certain on-demand DB instances in your account. Discounts for reserved DB instances are tied to instance type and AWS Region.

The general process for working with reserved DB instances is: First get information about available reserved DB instance offerings, then purchase a reserved DB instance offering, and finally get information about your existing reserved DB instances.

Overview of reserved DB instances

When you purchase a reserved DB instance in Amazon RDS, you purchase a commitment to getting a discounted rate, on a specific DB instance type, for the duration of the reserved DB instance. To use an Amazon RDS reserved DB instance, you create a new DB instance just like you do for an on-demand instance. The new DB instance that you create must match the specifications of the reserved DB instance. If the specifications of the new DB instance match an existing reserved DB instance for your account, you are billed at the discounted rate offered for the reserved DB instance. Otherwise, the DB instance is billed at an on-demand rate.

You can modify a reserved DB instance. If the modification is within the specifications of the reserved DB instance, part or all of the discount still applies to the modified DB instance. If the modification is outside the specifications, such as changing the instance class, the discount no longer applies. For more information, see [Size-flexible reserved DB instances \(p. 141\)](#).

For more information about reserved DB instances, including pricing, see [Amazon RDS reserved instances](#).

Offering types

Reserved DB instances are available in three varieties—No Upfront, Partial Upfront, and All Upfront—that let you optimize your Amazon RDS costs based on your expected usage.

No Upfront

This option provides access to a reserved DB instance without requiring an upfront payment. Your No Upfront reserved DB instance bills a discounted hourly rate for every hour within the term, regardless of usage, and no upfront payment is required. This option is only available as a one-year reservation.

Partial Upfront

This option requires a part of the reserved DB instance to be paid upfront. The remaining hours in the term are billed at a discounted hourly rate, regardless of usage. This option is the replacement for the previous Heavy Utilization option.

All Upfront

Full payment is made at the start of the term, with no other costs incurred for the remainder of the term regardless of the number of hours used.

If you are using consolidated billing, all the accounts in the organization are treated as one account. This means that all accounts in the organization can receive the hourly cost benefit of reserved DB instances that are purchased by any other account. For more information about consolidated billing, see [Amazon RDS reserved DB instances](#) in the *AWS Billing and Cost Management User Guide*.

Size-flexible reserved DB instances

When you purchase a reserved DB instance, one thing that you specify is the instance class, for example db.r5.large. For more information about instance classes, see [DB instance classes \(p. 10\)](#).

If you have a DB instance, and you need to scale it to larger capacity, your reserved DB instance is automatically applied to your scaled DB instance. That is, your reserved DB instances are automatically applied across all DB instance class sizes. Size-flexible reserved DB instances are available for DB instances with the same AWS Region and database engine. Size-flexible reserved DB instances can only scale in their instance class type. For example, a reserved DB instance for a db.r5.large can apply to a db.r5.xlarge, but not to a db.r6g.large, because db.r5 and db.r6g are different instance class types.

Reserved DB instance benefits also apply for both Multi-AZ and Single-AZ configurations. Flexibility means that you can move freely between configurations within the same DB instance class type. For example, you can move from a Single-AZ deployment running on one large DB instance (four normalized units) to a Multi-AZ deployment running on two small DB instances ($2 \times 2 = 4$ normalized units).

Size-flexible reserved DB instances are available for the following Amazon RDS database engines:

- MariaDB
- MySQL
- Oracle, Bring Your Own License
- PostgreSQL

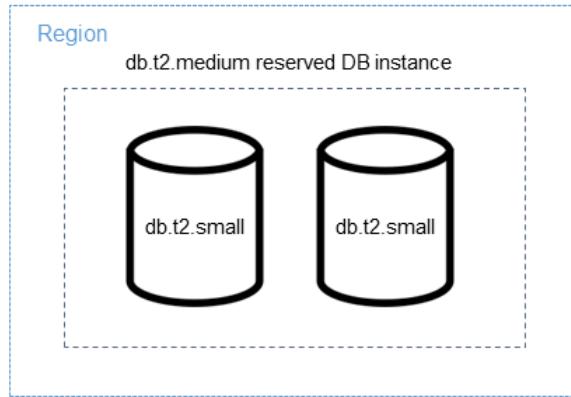
For details about using size-flexible reserved instances with Aurora, see [Reserved DB instances for Aurora](#).

You can compare usage for different reserved DB instance sizes by using normalized units. For example, one unit of usage on two db.r3.large DB instances is equivalent to eight normalized units of usage on one db.r3.small. The following table shows the number of normalized units for each DB instance size.

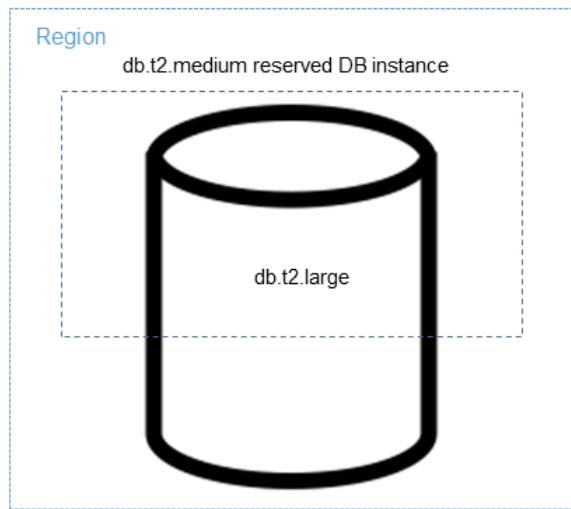
Instance size	Single-AZ normalized units	Multi-AZ normalized units
micro	0.5	1
small	1	2
medium	2	4
large	4	8
xlarge	8	16
2xlarge	16	32
4xlarge	32	64
6xlarge	48	96
8xlarge	64	128
10xlarge	80	160
12xlarge	96	192
16xlarge	128	256
24xlarge	192	384

Instance size	Single-AZ normalized units	Multi-AZ normalized units
32xlarge	256	512

For example, suppose that you purchase a db.t2.medium reserved DB instance, and you have two running db.t2.small DB instances in your account in the same AWS Region. In this case, the billing benefit is applied in full to both instances.



Alternatively, if you have one db.t2.large instance running in your account in the same AWS Region, the billing benefit is applied to 50 percent of the usage of the DB instance.



Reserved DB instance billing example

The price for a reserved DB instance doesn't include regular costs associated with storage, backups, and I/O. The following example illustrates the total cost per month for a reserved DB instance:

- An RDS for MySQL reserved Single-AZ db.r4.large DB instance class in US East (N. Virginia) with the No Upfront option at a cost of \$0.12 for the instance, or \$90 per month
- 400 GiB of General Purpose SSD (gp2) storage at a cost of 0.115 per GiB per month, or \$45.60 per month
- 600 GiB of backup storage at \$0.095, or \$19 per month (400 GiB free)

Add all of these options (\$90 + \$45.60 + \$19) with the reserved DB instance, and the total cost per month is \$154.60.

If you chose to use an on-demand DB instance instead of a reserved DB instance, an RDS for MySQL Single-AZ db.r4.large DB instance class in US East (N. Virginia) costs \$0.1386 per hour, or \$101.18 per month. So, for an on-demand DB instance, add all of these options (\$101.18 + \$45.60 + \$19), and the total cost per month is \$165.78. You save a little over \$11 per month by using the reserved DB instance.

Note

The prices in this example are sample prices and might not match actual prices. For Amazon RDS pricing information, see the [Amazon RDS product page](#).

Deleting a reserved DB instance

The terms for a reserved DB instance involve a one-year or three-year commitment. You can't cancel a reserved DB instance. However, you can delete a DB instance that is covered by a reserved DB instance discount. The process for deleting a DB instance that is covered by a reserved DB instance discount is the same as for any other DB instance.

You're billed for the upfront costs regardless of whether you use the resources.

If you delete a DB instance that is covered by a reserved DB instance discount, you can launch another DB instance with compatible specifications. In this case, you continue to get the discounted rate during the reservation term (one or three years).

Working with reserved DB instances

You can use the AWS Management Console, the AWS CLI, and the RDS API to work with reserved DB instances.

Console

You can use the AWS Management Console to work with reserved DB instances as shown in the following procedures.

To get pricing and information about available reserved DB instance offerings

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Reserved instances**.
3. Choose **Purchase Reserved DB Instance**.
4. For **Product description**, choose the DB engine and licensing type.
5. For **DB instance class**, choose the DB instance class.
6. For **Deployment Option**, choose whether you want a Multi-AZ deployment.
7. For **Term**, choose the length of time you want the DB instance reserved.
8. For **Offering type**, choose the offering type.

After you select the offering type, you can see the pricing information.

Important

Choose **Cancel** to avoid purchasing the reserved DB instance and incurring any charges.

After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering as shown in the following procedure.

To purchase a reserved DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Reserved instances**.

3. Choose **Purchase reserved DB instance**.

4. For **Product description**, choose the DB engine and licensing type.

5. For **DB instance class**, choose the DB instance class.

6. For **Multi-AZ deployment**, choose whether you want a Multi-AZ deployment.

7. For **Term**, choose the length of time you want the DB instance reserved.

8. For **Offering type**, choose the offering type.

After you choose the offering type, you can see the pricing information.

9. (Optional) You can assign your own identifier to the reserved DB instances that you purchase to help you track them. For **Reserved Id**, type an identifier for your reserved DB instance.

10. Choose **Submit**.

Your reserved DB instance is purchased, then displayed in the **Reserved instances** list.

After you have purchased reserved DB instances, you can get information about your reserved DB instances as shown in the following procedure.

To get information about reserved DB instances for your AWS account

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the Navigation pane, choose **Reserved instances**.

The reserved DB instances for your account appear. To see detailed information about a particular reserved DB instance, choose that instance in the list. You can then see detailed information about that instance in the detail pane at the bottom of the console.

AWS CLI

You can use the AWS CLI to work with reserved DB instances as shown in the following examples.

Example of getting available reserved DB instance offerings

To get information about available reserved DB instance offerings, call the AWS CLI command `describe-reserved-db-instances-offerings`.

```
aws rds describe-reserved-db-instances-offerings
```

This call returns output similar to the following:

OFFERING	OfferingId	Class	Multi-AZ	Duration	Fixed
Price	Usage Price	Description	Offering Type		
OFFERING	438012d3-4052-4cc7-b2e3-8d3372e0e706	db.r3.large	y	1y	1820.00
USD	0.368	USD mysql	Partial Upfront		
OFFERING	649fd0c8-cf6d-47a0-bfa6-060f8e75e95f	db.r3.small	n	1y	227.50
USD	0.046	USD mysql	Partial Upfront		
OFFERING	123456cd-ab1c-47a0-bfa6-12345667232f	db.r3.small	n	1y	162.00
USD	0.00	USD mysql	All Upfront		
Recurring Charges:		Amount	Currency	Frequency	
Recurring Charges:		0.123	USD	Hourly	

OFFERING	123456cd-ab1c-37a0-bfa6-12345667232d	db.r3.large	y	1y	700.00
USD	0.00 USD	mysql	All	Upfront	
Recurring Charges:	Amount	Currency	Frequency		
Recurring Charges:	1.25	USD	Hourly		
OFFERING	123456cd-ab1c-17d0-bfa6-12345667234e	db.r3.xlarge	n	1y	4242.00
USD	2.42 USD	mysql	No	Upfront	

After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering.

To purchase a reserved DB instance, use the AWS CLI command [purchase-reserved-db-instances-offering](#) with the following parameters:

- **--reserved-db-instances-offering-id** – The ID of the offering that you want to purchase. See the preceding example to get the offering ID.
- **--reserved-db-instance-id** – You can assign your own identifier to the reserved DB instances that you purchase to help track them.

Example of purchasing a reserved DB instance

The following example purchases the reserved DB instance offering with ID **649fd0c8-cf6d-47a0-bfa6-060f8e75e95f**, and assigns the identifier of **MyReservation**.

For Linux, macOS, or Unix:

```
aws rds purchase-reserved-db-instances-offering \
--reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f \
--reserved-db-instance-id MyReservation
```

For Windows:

```
aws rds purchase-reserved-db-instances-offering ^
--reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f ^
--reserved-db-instance-id MyReservation
```

The command returns output similar to the following:

RESERVATION	ReservationId	Class	Multi-AZ	Start Time	Duration
Fixed Price	Usage Price	Count	State	Description	Offering Type
RESERVATION	MyReservation	db.r3.small	y	2011-12-19T00:30:23.247Z	1y
455.00	USD	0.092	1	payment-pending	mysql Partial Upfront

After you have purchased reserved DB instances, you can get information about your reserved DB instances.

To get information about reserved DB instances for your AWS account, call the AWS CLI command [describe-reserved-db-instances](#), as shown in the following example.

Example of getting your reserved DB instances

```
aws rds describe-reserved-db-instances
```

The command returns output similar to the following:

RESERVATION	ReservationId	Class	Multi-AZ	Start Time	Duration
Fixed Price	Usage Price	Count	State	Description	Offering Type
RESERVATION	MyReservation	db.r3.small	y	2011-12-09T23:37:44.720Z	1y
455.00	USD	0.092	1	retired	mysql Partial Upfront

RDS API

You can use the RDS API to work with reserved DB instances:

- To get information about available reserved DB instance offerings, call the Amazon RDS API operation [DescribeReservedDBInstancesOfferings](#).
 - After you have information about the available reserved DB instance offerings, you can use the information to purchase an offering. Call the [PurchaseReservedDBInstancesOffering](#) RDS API operation with the following parameters:
 - `--reserved-db-instances-offering-id` – The ID of the offering that you want to purchase.
 - `--reserved-db-instance-id` – You can assign your own identifier to the reserved DB instances that you purchase to help track them.
 - After you have purchased reserved DB instances, you can get information about your reserved DB instances. Call the [DescribeReservedDBInstances](#) RDS API operation.

Viewing the billing for your reserved DB instances

You can view the billing for your reserved DB instances in the Billing Dashboard in the AWS Management Console.

To view reserved DB instance billing

1. Sign in to the AWS Management Console.
 2. From the **account menu** at the upper right, choose **Billing Dashboard**.
 3. Choose **Bill Details** at the upper right of the dashboard.
 4. Under **AWS Service Charges**, expand **Relational Database Service**.
 5. Expand the AWS Region where your reserved DB instances are, for example **US West (Oregon)**.

Your reserved DB instances and their hourly charges for the current month are shown under **Amazon Relational Database Service for Database Engine Reserved Instances**.



The reserved DB instance in this example was purchased All Upfront, so there are no hourly charges.

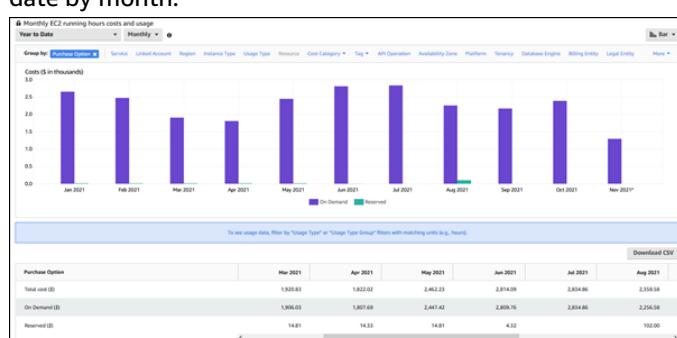
- 6 Choose the **Cost Explorer** (bar graph) icon next to the **Reserved Instances** heading.

The Cost Explorer displays the **Monthly EC2 running hours costs and usage** graph.

7. Clear the **Usage Type Group** filter to the right of the graph.

- 8 Choose the time period and time unit for which you want to examine usage costs

The following example shows usage costs for on-demand and reserved DB instances for the year to date by month.



The reserved DB instance costs from January through June 2021 are monthly charges for a Partial Upfront instance, while the cost in August 2021 is a one-time charge for an All Upfront instance.

The reserved instance discount for the Partial Upfront instance expired in June 2021, but the DB instance wasn't deleted. After the expiration date, it was simply charged at the on-demand rate.

Setting up for Amazon RDS

Before you use Amazon Relational Database Service for the first time, complete the following tasks.

Topics

- [Sign up for an AWS account \(p. 148\)](#)
- [Create an administrative user \(p. 148\)](#)
- [Create IAM user access keys \(p. 149\)](#)
- [Determine requirements \(p. 150\)](#)
- [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#)

If you already have an AWS account, know your Amazon RDS requirements, and prefer to use the defaults for IAM and VPC security groups, skip ahead to [Getting started with Amazon RDS \(p. 153\)](#).

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, [assign administrative access to an administrative user](#), and use only the root user to perform [tasks that require root user access](#).

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to <https://aws.amazon.com/> and choosing **My Account**.

Create an administrative user

After you sign up for an AWS account, create an administrative user so that you do not use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the [AWS Management Console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.
For help signing in using root user, see [Signing in as the root user](#) in the *AWS Sign-In User Guide*.
2. Turn on multi-factor authentication (MFA) for your root user.

For instructions, see [Enable a virtual MFA device for your AWS account root user \(console\)](#) in the *IAM User Guide*.

Create an administrative user

- For your daily administrative tasks, assign administrative access to an administrative user in AWS IAM Identity Center (successor to AWS Single Sign-On).

For instructions, see [Getting started](#) in the *AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide*.

Sign in as the administrative user

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

For help signing in using an IAM Identity Center user, see [Signing in to the AWS access portal](#) in the *AWS Sign-In User Guide*.

Create IAM user access keys

Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS. If you don't have access keys, you can create them from the AWS Management Console. As a best practice, do not use the AWS account root user access keys for any task where it's not required. Instead, [create a new administrator IAM user](#) with access keys for yourself.

The only time that you can view or download the secret access key is when you create the keys. You cannot recover them later. However, you can create new access keys at any time. You must also have permissions to perform the required IAM actions. For more information, see [Permissions required to access IAM resources](#) in the *IAM User Guide*.

To create access keys for an IAM user

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
 2. In the navigation pane, choose **Users**.
 3. Choose the name of the user whose access keys you want to create, and then choose the **Security credentials** tab.
 4. In the **Access keys** section, choose **Create access key**.
 5. To view the new access key pair, choose **Show**. You will not have access to the secret access key again after this dialog box closes. Your credentials will look something like this:
 - Access key ID: AKIAIOSFODNN7EXAMPLE
 - Secret access key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
 6. To download the key pair, choose **Download .csv file**. Store the keys in a secure location. You will not have access to the secret access key again after this dialog box closes.
 7. After you download the .csv file, choose **Close**. When you create an access key, the key pair is active by default, and you can use the pair right away.
- Keep the keys confidential in order to protect your AWS account and never email them. Do not share them outside your organization, even if an inquiry appears to come from AWS or Amazon.com. No one who legitimately represents Amazon will ever ask you for your secret key.

Related topics

- [What is IAM? in the IAM User Guide](#)
- [AWS security credentials in AWS General Reference](#)

Determine requirements

The basic building block of Amazon RDS is the DB instance. In a DB instance, you create your databases. A DB instance provides a network address called an *endpoint*. Your applications use this endpoint to connect to your DB instance. When you create a DB instance, you specify details like storage, memory, database engine and version, network configuration, security, and maintenance periods. You control network access to a DB instance through a security group.

Before you create a DB instance and a security group, you must know your DB instance and network needs. Here are some important things to consider:

- **Resource requirements** – What are the memory and processor requirements for your application or service? You use these settings to help you determine what DB instance class to use. For specifications about DB instance classes, see [DB instance classes \(p. 10\)](#).
- **VPC, subnet, and security group** – Your DB instance will most likely be in a virtual private cloud (VPC). To connect to your DB instance, you need to set up security group rules. These rules are set up differently depending on what kind of VPC you use and how you use it. For example, you can use: a default VPC or a user-defined VPC.

The following list describes the rules for each VPC option:

- **Default VPC** – If your AWS account has a default VPC in the current AWS Region, that VPC is configured to support DB instances. If you specify the default VPC when you create the DB instance, do the following:
 - Make sure to create a *VPC security group* that authorizes connections from the application or service to the Amazon RDS DB instance. Use the **Security Group** option on the VPC console or the AWS CLI to create VPC security groups. For information, see [Step 3: Create a VPC security group \(p. 2114\)](#).
 - Specify the default DB subnet group. If this is the first DB instance you have created in this AWS Region, Amazon RDS creates the default DB subnet group when it creates the DB instance.
- **User-defined VPC** – If you want to specify a user-defined VPC when you create a DB instance, be aware of the following:
 - Make sure to create a *VPC security group* that authorizes connections from the application or service to the Amazon RDS DB instance. Use the **Security Group** option on the VPC console or the AWS CLI to create VPC security groups. For information, see [Step 3: Create a VPC security group \(p. 2114\)](#).
 - The VPC must meet certain requirements in order to host DB instances, such as having at least two subnets, each in a separate Availability Zone. For information, see [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#).
 - Make sure to specify a DB subnet group that defines which subnets in that VPC can be used by the DB instance. For information, see the DB subnet group section in [Working with a DB instance in a VPC \(p. 2104\)](#).
- **High availability** – Do you need failover support? On Amazon RDS, a Multi-AZ deployment creates a primary DB instance and a secondary standby DB instance in another Availability Zone for failover support. We recommend Multi-AZ deployments for production workloads to maintain high availability. For development and test purposes, you can use a deployment that isn't Multi-AZ. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).
- **IAM policies** – Does your AWS account have policies that grant the permissions needed to perform Amazon RDS operations? If you are connecting to AWS using IAM credentials, your IAM account must

have IAM policies that grant the permissions required to perform Amazon RDS operations. For more information, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

- **Open ports** – What TCP/IP port does your database listen on? The firewalls at some companies might block connections to the default port for your database engine. If your company firewall blocks the default port, choose another port for the new DB instance. When you create a DB instance that listens on a port you specify, you can change the port by modifying the DB instance.
- **AWS Region** – What AWS Region do you want your database in? Having your database in close proximity to your application or web service can reduce network latency. For more information, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).
- **DB disk subsystem** – What are your storage requirements? Amazon RDS provides three storage types:
 - General Purpose (SSD)
 - Provisioned IOPS (PIOPS)
 - Magnetic (also known as standard storage)

For more information on Amazon RDS storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

When you have the information you need to create the security group and the DB instance, continue to the next step.

Provide access to your DB instance in your VPC by creating a security group

VPC security groups provide access to DB instances in a VPC. They act as a firewall for the associated DB instance, controlling both inbound and outbound traffic at the DB instance level. DB instances are created by default with a firewall and a default security group that protect the DB instance.

Before you can connect to your DB instance, you must add rules to a security group that enable you to connect. Use your network and configuration information to create rules to allow access to your DB instance.

For example, suppose that you have an application that accesses a database on your DB instance in a VPC. In this case, you must add a custom TCP rule that specifies the port range and IP addresses that your application uses to access the database. If you have an application on an Amazon EC2 instance, you can use the security group that you set up for the Amazon EC2 instance.

You can configure connectivity between an Amazon EC2 instance and a DB instance when you create the DB instance. For more information, see [Configure automatic network connectivity with an EC2 instance \(p. 230\)](#).

Tip

You can set up network connectivity between an Amazon EC2 instance and a DB instance automatically when you create the DB instance. For more information, see [Configure automatic network connectivity with an EC2 instance \(p. 230\)](#).

For information about common scenarios for accessing a DB instance, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

To create a VPC security group

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc>.

Note

Make sure you are in the VPC console, not the RDS console.

2. In the upper-right corner of the AWS Management Console, choose the AWS Region where you want to create your VPC security group and DB instance. In the list of Amazon VPC resources for that AWS Region, you should see at least one VPC and several subnets. If you don't, you don't have a default VPC in that AWS Region.
3. In the navigation pane, choose **Security Groups**.
4. Choose **Create security group**.
The **Create security group** page appears.
5. In **Basic details**, enter the **Security group name** and **Description**. For **VPC**, choose the VPC that you want to create your DB instance in.
6. In **Inbound rules**, choose **Add rule**.
 - a. For **Type**, choose **Custom TCP**.
 - b. For **Port range**, enter the port value to use for your DB instance.
 - c. For **Source**, choose a security group name or type the IP address range (CIDR value) from where you access the DB instance. If you choose **My IP**, this allows access to the DB instance from the IP address detected in your browser.
7. If you need to add more IP addresses or different port ranges, choose **Add rule** and enter the information for the rule.
8. (Optional) In **Outbound rules**, add rules for outbound traffic. By default, all outbound traffic is allowed.
9. Choose **Create security group**.

You can use the VPC security group that you just created as the security group for your DB instance when you create it.

Note

If you use a default VPC, a default subnet group spanning all of the VPC's subnets is created for you. When you create a DB instance, you can select the default VPC and use **default** for **DB Subnet Group**.

After you have completed the setup requirements, you can create a DB instance using your requirements and security group. To do so, follow the instructions in [Creating an Amazon RDS DB instance \(p. 230\)](#). For information about getting started by creating a DB instance that uses a specific DB engine, see the relevant documentation in the following table.

Database engine	Documentation
MariaDB	Creating a MariaDB DB instance and connecting to a database on a MariaDB DB instance (p. 154)
Microsoft SQL Server	Creating a Microsoft SQL Server DB instance and connecting to it (p. 162)
MySQL	Creating a MySQL DB instance and connecting to a database on a MySQL DB instance (p. 172)
Oracle	Creating an Oracle DB instance and connecting to a database on an Oracle DB instance (p. 180)
PostgreSQL	Creating a PostgreSQL DB instance and connecting to a database on a PostgreSQL DB instance (p. 187)

Note

If you can't connect to a DB instance after you create it, see the troubleshooting information in [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Getting started with Amazon RDS

In the following examples, you can find how to create and connect to a DB instance using Amazon Relational Database Service (Amazon RDS). You can create a DB instance that uses MariaDB, MySQL, Microsoft SQL Server, Oracle, or PostgreSQL.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

Creating a DB instance and connecting to a database on a DB instance is slightly different for each of the DB engines. Choose one of the following DB engines that you want to use for detailed information on creating and connecting to the DB instance. After you have created and connected to your DB instance, there are instructions to help you delete the DB instance.

Topics

- [Creating a MariaDB DB instance and connecting to a database on a MariaDB DB instance \(p. 154\)](#)
- [Creating a Microsoft SQL Server DB instance and connecting to it \(p. 162\)](#)
- [Creating a MySQL DB instance and connecting to a database on a MySQL DB instance \(p. 172\)](#)
- [Creating an Oracle DB instance and connecting to a database on an Oracle DB instance \(p. 180\)](#)
- [Creating a PostgreSQL DB instance and connecting to a database on a PostgreSQL DB instance \(p. 187\)](#)
- [Tutorial: Create a web server and an Amazon RDS DB instance \(p. 198\)](#)

Creating a MariaDB DB instance and connecting to a database on a MariaDB DB instance

The easiest way to create a MariaDB DB instance is to use the AWS Management Console. After you create the DB instance, you can connect to a database on the DB instance. To do so, you can use command line tools such as mysql or graphical tools such as HeidiSQL.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

Topics

- [Creating a MariaDB DB instance \(p. 154\)](#)
- [Connecting to a database on a DB instance running the MariaDB database engine \(p. 158\)](#)
- [Deleting a DB instance \(p. 161\)](#)

Creating a MariaDB DB instance

The basic building block of Amazon RDS is the DB instance. This environment is where you run your MariaDB databases.

You can use **Easy create** to create a DB instance running MariaDB with the AWS Management Console. With **Easy create**, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default settings for the other configuration options. When you use **Standard create** instead of **Easy create**, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

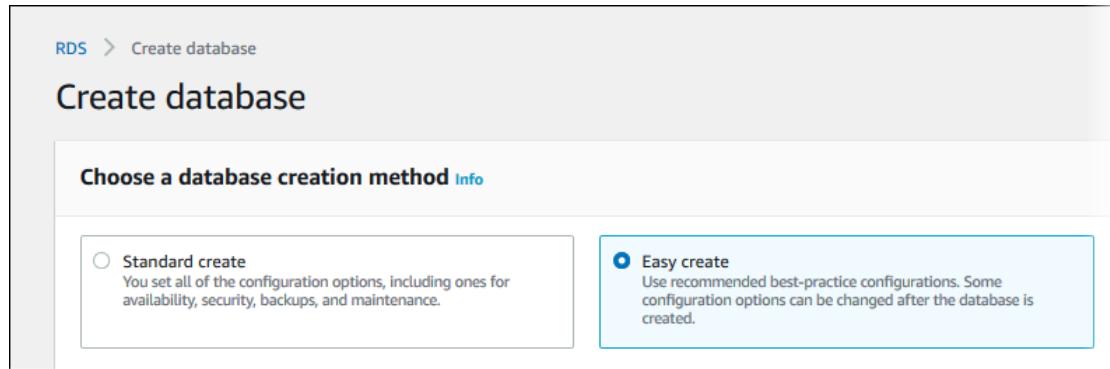
In this example, you use **Easy create** to create a DB instance running the MariaDB database engine with a db.t2.micro DB instance class.

Note

For information about creating DB instances with **Standard create**, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

To create a MariaDB DB instance with **Easy create**

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database** and make sure that **Easy create** is chosen.



5. In **Configuration**, choose **MariaDB**.
6. For **DB instance size**, choose **Free tier**.
7. For **DB instance identifier**, enter a name for the DB instance, or leave the default name.
8. For **Master username**, enter a name for the master user, or leave the default name.

The **Create database** page should look similar to the following image.

Create database

Choose a database creation method [Info](#)

Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type [Info](#)

Amazon Aurora



MySQL



MariaDB



PostgreSQL



Oracle



Microsoft SQL Server



DB instance size

Production

db.r6g.xlarge
4 vCPUs
32 GiB RAM
500 GiB

Dev/Test

db.r6g.large
2 vCPUs
16 GiB RAM
100 GiB

Free tier

db.t2.micro
1 vCPUs
1 GiB RAM
20 GiB

DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username [Info](#)

Type a login ID for the master user of your DB instance.

9. To use an automatically generated master password for the DB instance, make sure that the **Auto generate a password** box is selected.

To enter your master password, clear the **Auto generate a password** box, and then enter the same password in **Master password** and **Confirm password**.

10. (Optional) Open **View default settings for Easy create**.

▼ **View default settings for Easy create**

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use [Standard Create](#).

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-6594f31c)	No
Option Group	default:mariadb-10-4	Yes
Subnet Group	default	Yes
Automatic Backups	Enabled	Yes
VPC Security Group	sg-68184619	Yes
Publically Accessible	No	Yes
Database Port	3306	Yes
DB Instance Identifier	database-1	Yes
DB Engine Version	10.4.13	Yes
DB Parameter Group	default.mariadb10.4	Yes
Performance Insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto Minor Version Upgrade Enabled	Yes
Delete Protection	Not Enabled	Yes

You can examine the default settings used with **Easy create**. The **Editable after database is created** column shows which options you can change after database creation.

- To change settings with **No** in that column, use **Standard create**.
- To change settings with **Yes** in that column, either use **Standard create**, or modify the DB instance after it is created to change the settings.

The following are important considerations for changing the default settings:

- In some cases, you might want your DB instance to use a specific virtual private cloud (VPC) based on the Amazon VPC service. Or you might require a specific subnet group or security group. If so, use **Standard create** to specify these resources. You might have created these resources when you set up for Amazon RDS. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

- If you want to be able to access the DB instance from a client outside of its VPC, use **Standard create** to set **Public access** to **Yes**.

If the DB instance should be private, leave **Public access** set to **No**.

11. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it.

If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

12. For **Databases**, choose the name of the new Maria DB instance.

On the RDS console, the details for new DB instance appear. The DB instance has a status of **Creating** until the DB instance is ready to use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new instance is available.

database-1			
Summary			
DB identifier	CPU	Info	Class
database-1		Creating	db.t2.micro
Role	Current activity	Engine	Region & AZ
Instance		MariaDB	-

[Connectivity & security](#) | [Monitoring](#) | [Logs & events](#) | [Configuration](#) | [Maintenance & backups](#) | [Tags](#)

Connecting to a database on a DB instance running the MariaDB database engine

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to a database on the DB instance. In this example, you connect to a database on a Maria DB instance using the mysql command-line tool. For more information on using MariaDB, see the [MariaDB documentation](#).

To connect to a database on a DB instance using the mysql command-line tool

1. Install a SQL client that you can use to connect to the DB instance.

You can connect to an Amazon RDS for MariaDB DB instance by using tools such as the mysql command-line client. For more information on using the mysql command-line client, see [mysql command-line client](#) in the MariaDB documentation. One GUI-based application that you can use

to connect is Heidi. For more information, see the [Download HeidiSQL](#) page. For information about installing MySQL (including the mysql command-line client), see [Installing and upgrading MySQL](#).

2. Make sure that your DB instance is associated with a security group that provides access to it. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

If you didn't specify the appropriate security group when you created the DB instance, you can modify the DB instance to change its security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If your DB instance is publicly accessible, make sure its associated security group has inbound rules for the IP addresses that you want to access it. If your DB instance is private, make sure its associated security group has inbound rules for the security group of each resource to access it. An example is the security group for an Amazon EC2 instance.

3. Find the endpoint (DNS name) and port number for your DB instance.
 - a. Open the RDS console and then choose **Databases** to display a list of your DB instances.
 - b. Choose the Maria DB instance name to display its details.
 - c. On the **Connectivity & security** tab, copy the endpoint. Also note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the Amazon RDS console interface. At the top, the navigation path is RDS > Databases > mydb. Below this, the database name "mydb" is displayed in a large font. A "Summary" section provides basic information: DB identifier (mydb), Role (Instance), CPU usage (2.33%), and Current activity (0 Connections). Below the summary, there are tabs for Connectivity & security, Monitoring, Logs & events, and Configuration. The Connectivity & security tab is selected. Under this tab, the "Endpoint & port" section is highlighted with a red oval. It shows the Endpoint as "mydb. [REDACTED].us-east-1.rds.amazonaws.com" and the Port as "3306". To the right of the endpoint, there is a vertical column of network-related information: Network (Available), us-east-1, VPC (vpc-6E), and Subnet (default).

4. Enter the following command at a command prompt on a client computer to connect to a database on a Maria DB instance. Substitute the DNS name (endpoint) for your DB instance for <endpoint>. In addition, substitute the master user name that you used for <mymasteruser> and provide the master password that you used when prompted for a password.

```
PROMPT> mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

After you enter the password for the user, you should see output similar to the following.

```
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 31
```

```
Server version: 10.5.15-MariaDB-log Source distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

For more information about connecting to a MariaDB DB instance, see [Connecting to a DB instance running the MariaDB database engine \(p. 986\)](#). If you can't connect to your DB instance, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Deleting a DB instance

After you connect to the sample DB instance that you created, delete the DB instance so you're no longer charged for it.

To delete a DB instance with no final DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance you want to delete.
4. For **Actions**, choose **Delete**.
5. For **Create final snapshot?**, choose **No**, and select the acknowledgment.
6. Choose **Delete**.

Creating a Microsoft SQL Server DB instance and connecting to it

The basic building block of Amazon RDS is the DB instance. Your Amazon RDS DB instance is similar to your on-premises Microsoft SQL Server. After you create your SQL Server DB instance, you can add one or more custom databases to it.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

In this topic, you create a sample SQL Server DB instance. You then connect to the DB instance and run a simple query. Finally, you delete the sample DB instance.

Creating a sample SQL Server DB instance

You can use **Easy create** to create a DB instance running Microsoft SQL Server with the AWS Management Console. With **Easy create**, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default settings for the other configuration options. When you use **Standard create** instead of **Easy create**, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

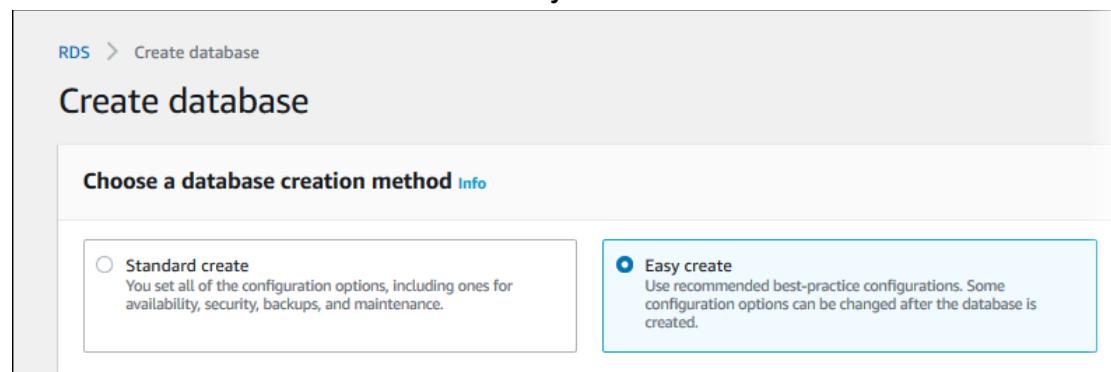
In this example, you use **Easy create** to create a DB instance running the Microsoft SQL Server database engine with a db.t2.micro DB instance class.

Note

For information about creating DB instances with **Standard create**, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

To create a Microsoft SQL Server DB instance with Easy create

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database** and make sure that **Easy create** is chosen.



5. From **Engine type**, choose **Microsoft SQL Server**.
6. For **DB instance size**, choose **Free tier**.
7. For **DB instance identifier**, enter **sample-instance**, or leave the default name.

8. For **Master username**, enter a name for the master user, or leave the default name.
9. To use an automatically generated master password for the DB instance, select the **Auto generate a password** box.

To enter your master password, clear the **Auto generate a password** box, and then enter the same password in **Master password** and **Confirm password**.

The **Create database** page should look similar to the following image.

Create database

Choose a database creation method [Info](#)

Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type [Info](#)

Amazon Aurora



MySQL



MariaDB



PostgreSQL



Oracle



Microsoft SQL Server



DB instance size

Production

db.r5.xlarge
4 vCPUs
32 GiB RAM
500 GiB
3.198 USD/hour

Dev/Test

db.m5.large
2 vCPUs
8 GiB RAM
100 GiB
0.993 USD/hour

Free tier

db.t2.micro
1 vCPUs
1 GiB RAM
20 GiB

DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

sample-instance

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username [Info](#)

10. (Optional) Expand **View default settings for Easy create.**

▼ View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use [Standard Create](#).

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	tutorial-vpc (vpc-0c55993b496995ef9)	No
Option Group	default:sqlserver-ex-14-00	Yes
Subnet Group	tutorial-db-subnet-group	Yes
Automatic Backups	Enabled	Yes
VPC Security Group	sg-087f3797a22d126d9	Yes
Publicly Accessible	No	Yes
Database Port	1433	Yes
DB Instance Identifier	sample-instance	Yes
DB Engine Version	14.00.3381.3.v1	Yes
DB Parameter Group	default.sqlserver-ex-14.0	Yes
Performance Insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto Minor Version Upgrade Enabled	Yes
Delete Protection	Not Enabled	Yes

You can examine the default settings used with **Easy create**. The **Editable after database is created** column shows which options you can change after database creation.

- To change settings with **No** in that column, use [Standard create](#).
- To change settings with **Yes** in that column, either use [Standard create](#), or modify the DB instance after it is created to change the settings.

The following are important considerations for changing the default settings:

- In some cases, you might want your DB instance to use a specific virtual private cloud (VPC) based on the Amazon VPC service. Or you might require a specific subnet group or security group. If so, use [Standard create](#) to specify these resources. You might have created these resources when you set up for Amazon RDS. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

- If you want to be able to access the DB instance from a client outside of its VPC, use **Standard create** to set **Public access** to **Yes**.

If the DB instance should be private, leave **Public access** set to **No**.

11. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it.

If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

12. For **Databases**, choose the name of the new Microsoft SQL Server DB instance.

On the RDS console, the details for new DB instance appear. The DB instance has a status of **Creating** until the DB instance is ready to use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new instance is available.

The screenshot shows the RDS console with the path 'RDS > Databases > sample-instance'. The main title is 'sample-instance'. On the right, there are 'Modify' and 'Actions' buttons. Below the title, there's a 'Summary' section with a table. The 'Status' column for the first row (DB identifier: sample-instance) is circled in red and shows 'Creating'. Other columns show CPU: -, Class: db.t2.micro, Role: Instance, Current activity: -, Engine: SQL Server Express Edition, and Region & AZ: us-east-2b. At the bottom, tabs for 'Connectivity & security' (which is selected), 'Monitoring', 'Logs & events', 'Configuration', 'Maintenance & backups', and 'Tags' are visible.

DB identifier	CPU	Status	Class
sample-instance	-	Creating	db.t2.micro
Role	Current activity	Engine	Region & AZ
Instance	-	SQL Server Express Edition	us-east-2b

Connecting to your sample SQL Server DB instance

In the following procedure, you connect to your sample DB instance by using Microsoft SQL Server Management Studio (SSMS).

Before you begin, your database should have a status of **Available**. If it has a status of **Creating** or **Backing-up**, wait until it shows **Available**. The status updates without requiring you to refresh the page. This process can take up to 20 minutes.

Also, make sure that you have SSMS installed. You can also connect to RDS for SQL Server by using a different tool, such as an add-in for your development environment or some other database tool. However, this tutorial only covers using SSMS. To download a standalone version of this SSMS, see [Download SQL Server Management Studio \(SSMS\)](#) in the Microsoft documentation.

To connect to a DB instance using SSMS

1. Make sure that your DB instance is associated with a security group that provides access to it. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

If you didn't specify the appropriate security group when you created the DB instance, you can modify the DB instance to change its security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If your DB instance is publicly accessible, make sure its associated security group has inbound rules for the IP addresses that you want to access it. If your DB instance is private, make sure its associated security group has inbound rules for the security group of each resource to access it. An example is the security group for an Amazon EC2 instance.

2. Find the DNS name and port number for your DB instance.
 - a. Open the RDS console, and then choose **Databases** to display a list of your DB instances.
 - b. Hover your mouse cursor over the name **sample-instance**, which is blue. When you do this, the mouse cursor changes into a selection icon (for example, a pointing hand). Also, the DB instance name becomes underlined.

Click on the DB instance name to choose it. The screen changes to display the information for the DB instance you choose.

- c. On the **Connectivity** tab, which opens by default, copy the endpoint. The **Endpoint** looks something like this: `sample-instance.123456789012.us-east-2.rds.amazonaws.com`. Also, note the port number. The default port for SQL Server is 1433. If yours is different, write it down.

The screenshot shows the Amazon RDS console interface. At the top, the navigation path is RDS > Databases > sample-instance. Below this, the database name "sample-instance" is displayed in large bold letters. A "Summary" section provides key metrics: DB identifier (sample-instance), CPU usage (44.50%), Role (Instance), and Current activity (0 Connect). Below the summary, there are three tabs: Connectivity & security (selected), Monitoring, and Logs & events. The Connectivity & security tab displays the endpoint and port information, which is circled in red.

DB identifier	CPU
sample-instance	44.50%

Role	Current activity
Instance	0 Connect

Connectivity & security

Endpoint & port

Endpoint: sample-instance. .us-east-2.rds.amazonaws.com

Port: 1433

3. Start SQL Server Management Studio.

The **Connect to Server** dialog box appears.

4. Provide the following information for your sample DB instance:

a. For **Server type**, choose **Database Engine**.

b. For **Server name**, enter the DNS name, followed by a comma and the port number (the default port is 1433). For example, your server name should look like the following.

sample-instance.*abc2defghije.us-west-2.rds.amazonaws.com*,1433

c. For **Authentication**, choose **SQL Server Authentication**.

- d. For **Login**, enter the user name that you chose to use for your sample DB instance. This is also known as the master user name.
 - e. For **Password**, enter the password that you chose earlier for your sample DB instance. This is also known as the master user password.
5. Choose **Connect**.

After a few moments, SSMS connects to your DB instance.

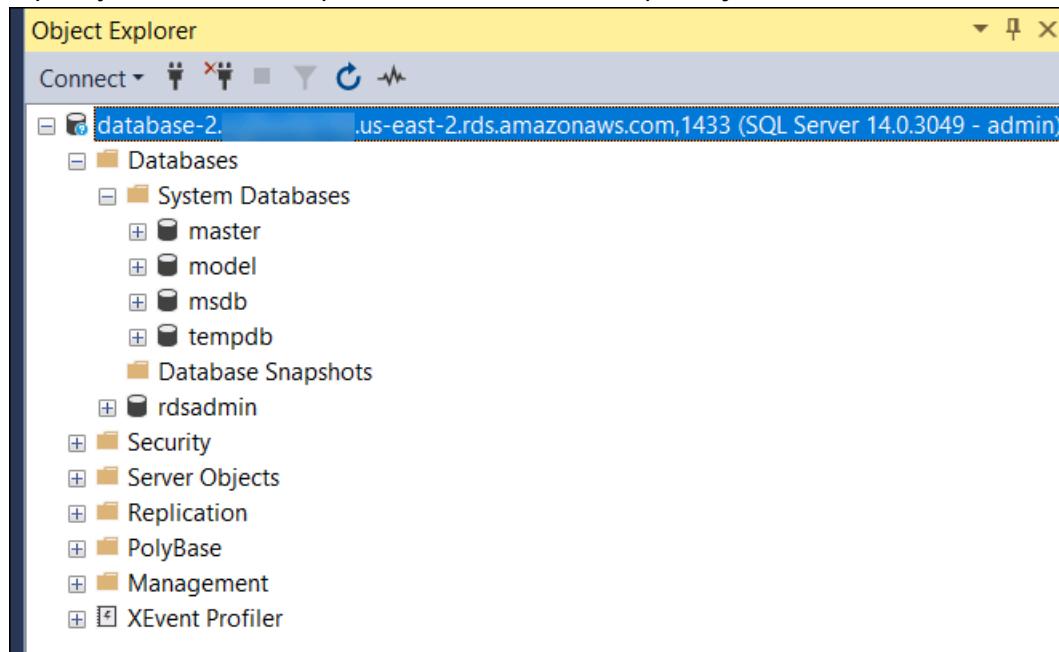
For more information about connecting to a Microsoft SQL Server DB instance, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#). For information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Exploring your sample SQL Server DB instance

In this procedure, you continue the previous procedure and explore your sample DB instance by using Microsoft SQL Server Management Studio (SSMS).

To explore a DB instance using SSMS

1. Your SQL Server DB instance comes with SQL Server's standard built-in system databases (master, model, msdb, and tempdb). To explore the system databases, do the following:
 - a. In SSMS, on the **View** menu, choose **Object Explorer**.
 - b. Expand your DB instance, expand **Databases**, and then expand **System Databases** as shown.



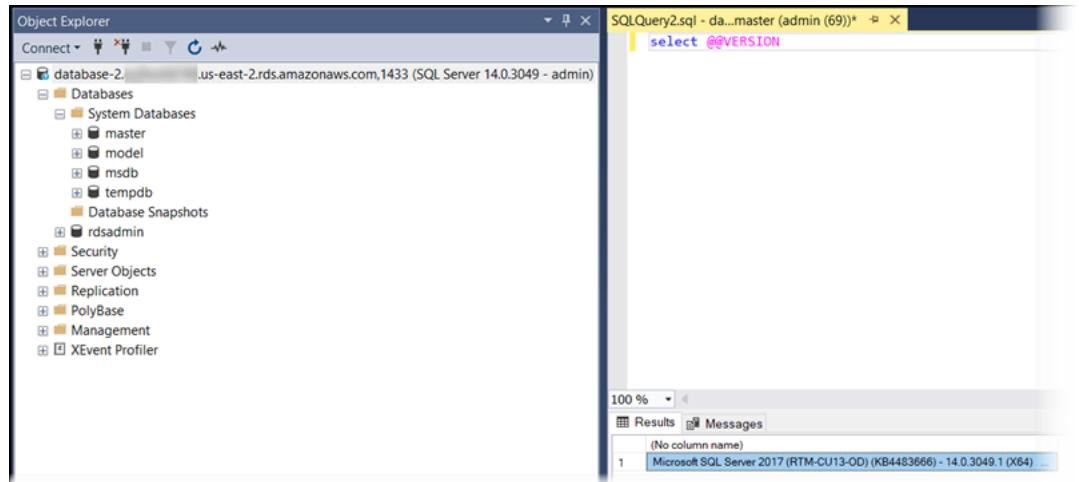
Your SQL Server DB instance also comes with a database named `rdsadmin`. Amazon RDS uses this database to store the objects that it uses to manage your database. The `rdsadmin` database also includes stored procedures that you can run to perform advanced tasks.

2. Start creating your own databases and running queries against your DB instance and databases as usual. To run a test query against your sample DB instance, do the following:
 - a. In SSMS, on the **File** menu point to **New** and then choose **Query with Current Connection**.

- b. Enter the following SQL query.

```
select @@VERSION
```

- c. Run the query. SSMS returns the SQL Server version of your Amazon RDS DB instance.



Deleting your sample DB instance

After you're done exploring your sample DB instance, delete it so that you're no longer charged for it.

To delete a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the button next to **sample-instance**, or whatever you named your sample DB instance.
4. From **Actions**, choose **Delete**.
5. If you see a message that says **This database has deletion protection option enabled**, follow these steps:
 - a. Choose **Modify**.
 - b. On the **Deletion protection** card (near the bottom of the page), clear the box next to **Enable deletion protection**. Then choose **Continue**.
 - c. On the **Scheduling of modifications** card, choose **Apply immediately**. Then choose **Modify DB instance**.
 - d. Try again to delete the instance by choosing **Delete** from the **Actions** menu.
6. Clear the box for **Create final snapshot**. Because this isn't a production database, you don't need to save a copy of it.
7. Verify that you selected the correct database to delete. The name "sample-instance" displays in the title of the screen: **Delete sample-instance instance?**

If you don't recognize the name of your sample instance in the title, choose **Cancel** and start over.
8. To confirm that you want to permanently delete the database that is displayed in the title of this screen, do the following:
 - Select the box to confirm: **I acknowledge that upon instance deletion, automated backups, including system snapshots and point-in-time recovery, will no longer be available.**

- Enter "**delete me**" into the box **To confirm deletion, type *delete me* into the field.**
- Choose **Delete**. This action can't be undone.

The database shows a status of **Deleting** until deletion is complete.

Creating a MySQL DB instance and connecting to a database on a MySQL DB instance

The easiest way to create a DB instance is to use the AWS Management Console. After you create the DB instance, you can use standard MySQL utilities such as MySQL Workbench to connect to a database on the DB instance.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

Topics

- [Creating a MySQL DB instance \(p. 172\)](#)
- [Connecting to a database on a DB instance running the MySQL database engine \(p. 176\)](#)
- [Deleting a DB instance \(p. 179\)](#)

Creating a MySQL DB instance

The basic building block of Amazon RDS is the DB instance. This environment is where you run your MySQL databases.

You can use **Easy create** to create a DB instance running MySQL with the AWS Management Console. With **Easy create**, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default settings for the other configuration options. When you use **Standard create** instead of **Easy create**, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

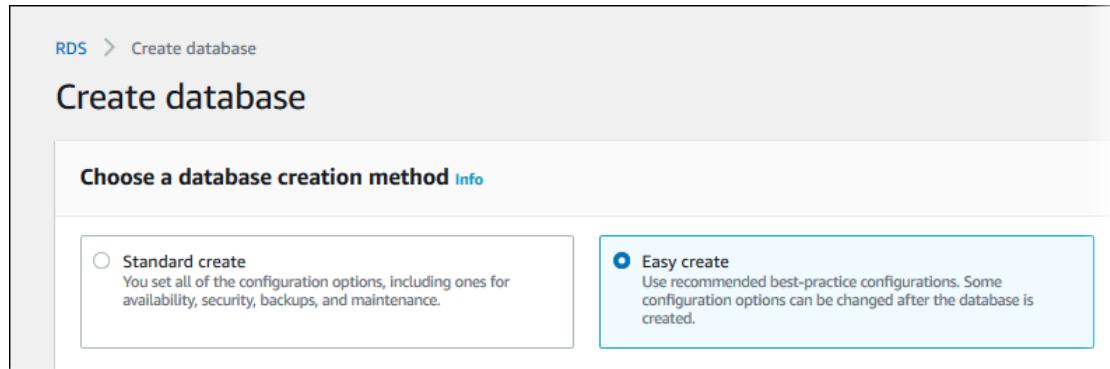
In this example, you use **Easy create** to create a DB instance running the MySQL database engine with a db.t2.micro DB instance class.

Note

For information about creating DB instances with **Standard create**, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

To create a MySQL DB instance with Easy create

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database** and make sure that **Easy create** is chosen.



5. In **Configuration**, choose **MySQL**.
6. For **DB instance size**, choose **Free tier**.
7. For **DB instance identifier**, enter a name for the DB instance, or leave the default name.
8. For **Master username**, enter a name for the master user, or leave the default name.

The **Create database** page should look similar to the following image.

Create database

Choose a database creation method [Info](#)

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type [Info](#)

Amazon Aurora 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

DB instance size

Production
db.r6g.xlarge
4 vCPUs
32 GiB RAM
500 GiB

Dev/Test
db.r6g.large
2 vCPUs
16 GiB RAM
100 GiB

Free tier
db.t2.micro
1 vCPUs
1 GiB RAM
20 GiB

DB instance identifier
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username [Info](#)
Type a login ID for the master user of your DB instance.

admin

9. To use an automatically generated master password for the DB instance, make sure that the **Auto generate a password** box is selected.

To enter your master password, clear the **Auto generate a password** box, and then enter the same password in **Master password** and **Confirm password**.

10. (Optional) Open **View default settings for Easy create**.

▼ View default settings for Easy create		
Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-6594f31c)	No
Option Group	default:mysql-8-0	Yes
Subnet Group	default	Yes
Automatic Backups	Enabled	Yes
VPC Security Group	sg-68184619	Yes
Publically Accessible	No	Yes
Database Port	3306	Yes
DB Instance Identifier	database-1	Yes
DB Engine Version	8.0.23	Yes
DB Parameter Group	default.mysql8.0	Yes
Performance Insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto Minor Version Upgrade Enabled	Yes
Delete Protection	Not Enabled	Yes

You can examine the default settings used with **Easy create**. The **Editable after database is created** column shows which options you can change after database creation.

- To change settings with **No** in that column, use **Standard create**.
- To change settings with **Yes** in that column, either use **Standard create**, or modify the DB instance after it is created to change the settings.

The following are important considerations for changing the default settings:

- In some cases, you might want your DB instance to use a specific virtual private cloud (VPC) based on the Amazon VPC service. Or you might require a specific subnet group or security group. If so,

use **Standard create** to specify these resources. You might have created these resources when you set up for Amazon RDS. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

- If you want to be able to access the DB instance from a client outside of its VPC, use **Standard create** to set **Public access** to **Yes**.

If the DB instance should be private, leave **Public access** set to **No**.

11. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

You can use the user name and password that appears to connect to the DB instance as the master user.

Important

You can't view the master user password again. If you don't record it, you might have to change it.

If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

12. In the **Databases** list, choose the name of the new MySQL DB instance.

On the RDS console, the details for new DB instance appear. The DB instance has a status of **Creating** until the DB instance is ready to use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new instance is available.

database-1		Modify	Actions ▾
Summary			
DB identifier database-1	CPU	Info 🕒 Creating	Class db.t2.micro
Role Instance	Current activity	Engine MySQL	Region & AZ -

Connecting to a database on a DB instance running the MySQL database engine

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to a database on the DB instance. In this example, you connect to a database on a MySQL DB instance using MySQL monitor commands.

To connect to a database on a DB instance using MySQL monitor

1. Install a SQL client that you can use to connect to the DB instance.

You can connect to a MySQL DB instance by using tools such as the mysql command line utility. For more information on using the MySQL client, see [mysql - the MySQL command-line client](#)

in the MySQL documentation. One GUI-based application that you can use to connect is MySQL Workbench. For more information, see the [Download MySQL Workbench](#) page.

For more information on using MySQL, see the [MySQL documentation](#). For information about installing MySQL (including the MySQL client), see [Installing and upgrading MySQL](#).

If your DB instance is publicly accessible, you can install the SQL client outside of your VPC. If your DB instance is private, you typically install the SQL client on a resource inside your VPC, such as an Amazon EC2 instance.

2. Make sure that your DB instance is associated with a security group that provides access to it. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

If you didn't specify the appropriate security group when you created the DB instance, you can modify the DB instance to change its security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If your DB instance is publicly accessible, make sure its associated security group has inbound rules for the IP addresses that you want to access it. If your DB instance is private, make sure its associated security group has inbound rules for the security group of each resource to access it. An example is the security group for an Amazon EC2 instance.

3. Find the endpoint (DNS name) and port number for your DB instance.
 - a. Open the RDS console and then choose **Databases** to display a list of your DB instances.
 - b. Choose the MySQL DB instance name to display its details.
 - c. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the Amazon RDS console interface. At the top, the navigation path is RDS > Databases > mydb. Below this, the database name "mydb" is displayed in a large font. A "Summary" section provides basic information: DB identifier (mydb), Role (Instance), CPU usage (2.33%), and Current activity (0 Connections). Below the summary, there are tabs for Connectivity & security, Monitoring, Logs & events, and Configuration. The Connectivity & security tab is selected. Under this tab, the "Endpoint & port" section is highlighted with a red oval. It shows the Endpoint as "mydb. [REDACTED].us-east-1.rds.amazonaws.com" and the Port as "3306". To the right of the endpoint, there is a vertical column of network-related information: Network (Available), us-east-1, VPC (vpc-6E), Subnet (default), and Default security group (not visible).

4. Connect to a database on a MySQL DB instance. For example, enter the following command at a command prompt on a client computer. By doing this, you connect to a database on a MySQL DB instance using the MySQL client.

Substitute the DNS name for your DB instance for `<endpoint>`. In addition, substitute the master user name that you used for `<mymasteruser>`, and provide the master password that you used when prompted for a password.

```
PROMPT> mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

After you enter the password for the user, you should see output similar to the following.

```
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 9738  
Server version: 8.0.23 Source distribution  
  
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.  
  
mysql>
```

For more information about connecting to a MySQL DB instance, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#). If you can't connect to your DB instance, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Deleting a DB instance

After you connect to and explore the sample DB instance that you created, delete it so you're no longer charged for it.

To delete a DB instance with no final DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to delete.
4. For **Actions**, choose **Delete**.
5. For **Create final snapshot?**, choose **No**, and select the acknowledgment.
6. Choose **Delete**.

Creating an Oracle DB instance and connecting to a database on an Oracle DB instance

The basic building block of Amazon RDS is the DB instance. Your Amazon RDS DB instance is similar to your on-premises Oracle database.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

There's no charge for creating an AWS account. However, by completing this tutorial, you might incur costs for the AWS resources that you use. You can delete these resources after you complete the tutorial if they are no longer needed.

In this topic, you create a sample Oracle DB instance and connect to it. Finally, you delete the sample DB instance.

Creating a sample Oracle DB instance

The DB instance is where you run your Oracle databases.

Note

RDS for Oracle supports a single-tenant architecture, where a pluggable database (PDB) resides in a multitenant container database (CDB). For more information, see [RDS for Oracle architecture \(p. 1480\)](#).

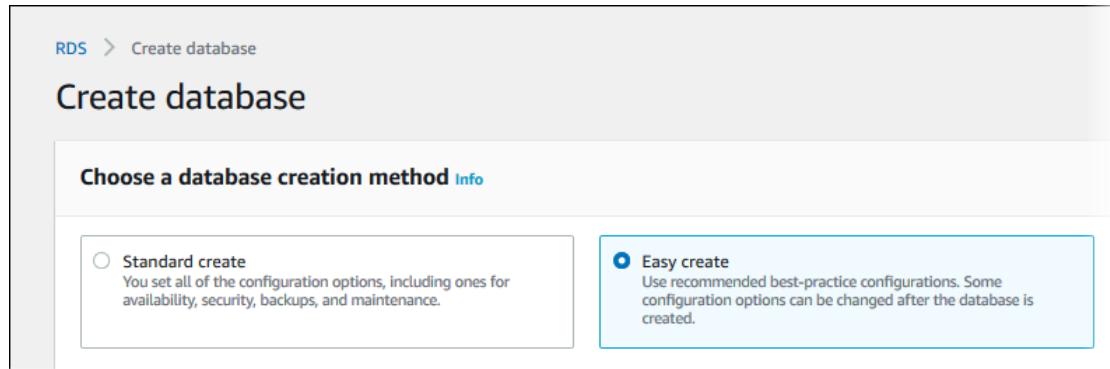
You can use **Easy create** to create a DB instance running Oracle with the AWS Management Console. With **Easy create**, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default settings for the other configuration options. When you use **Standard create** instead of **Easy create**, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

In this example, you use **Easy create** to create a DB instance running the Oracle database engine with a db.m4.large DB instance class.

For information about creating DB instances with **Standard create**, see [Creating an Amazon RDS DB instance \(p. 230\)](#). If you want to use free tier, use **Standard create**.

To create an Oracle DB instance with Easy create enabled

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database** and ensure that **Easy create** is chosen.



5. In **Configuration**, choose **Oracle**.
6. For **DB instance size**, choose **Free tier**. If **Free tier** isn't available, choose **Dev/Test**.
7. For **DB instance identifier**, enter a name for the DB instance, or leave the default name of **database-1**.
8. For **Master username**, enter a name for the master user, or leave the default name.

The **Create database** page should look similar to the following image.

Create database

Choose a database creation method [Info](#)

Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type [Info](#)

Amazon Aurora



MySQL



MariaDB



PostgreSQL



Oracle



Microsoft SQL Server



DB instance size

Production

db.r4.large
2 vCPUs
15.25 GiB RAM
500 GiB

Dev/Test

db.m4.large
2 vCPUs
8 GiB RAM
100 GiB

DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username [Info](#)

Type a login ID for the master user of your DB instance.

9. To use an automatically generated master password for the DB instance, make sure that the **Auto generate a password** box is selected.

To enter your master password, clear the **Auto generate a password** box, and then enter the same password in **Master password** and **Confirm password**.

10. (Optional) Open **View default settings for Easy create**.

▼ View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use [Standard Create](#).

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-2aed394c)	No
Option Group	default:oracle-se2-19	Yes
Subnet Group	default	Yes
Automatic Backups	Enabled	Yes
VPC Security Group	sg-0b4ff871	Yes
Publically Accessible	No	Yes
Database Port	1521	Yes
DB Instance Identifier	database-1	Yes
DB Engine Version	19.0.0.0.ru-2021-04.rur-2021-04.r1	Yes
DB Parameter Group	default.oracle-se2-19	Yes
Performance Insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto Minor Version Upgrade Enabled	Yes
Delete Protection	Not Enabled	Yes

You can examine the default settings used with **Easy create**. The **Editable after database is created** column shows which options you can change after database creation.

- To change settings with **No** in that column, use [Standard create](#).
- To change settings with **Yes** in that column, either use [Standard create](#), or modify the DB instance after it is created to change the settings.

The following are important considerations for changing the default settings:

- In some cases, you might want your DB instance to use a specific virtual private cloud (VPC) based on the Amazon VPC service. Or you might require a specific subnet group or security group. If so, use [Standard create](#) to specify these resources. You might have created these resources when you set up for Amazon RDS. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

- If you want to be able to access the DB instance from a client outside of its VPC, use **Standard create** to set **Public access** to **Yes**.

If the DB instance should be private, leave **Public access** set to **No**.

- If you want to use free tier, use **Standard create** to set the Oracle version lower than version 12.2, and then choose **Free tier** in **Templates**.

11. Choose **Create database**.

If you used an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it.

If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

12. For **Databases**, choose the name of the new Oracle DB instance.

On the RDS console, the details for new DB instance appear. The DB instance has a status of **Creating** until the DB instance is ready to use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new instance is available.

database-1				Modify	Actions ▾
Summary					
DB identifier database-1	CPU	Info  Creating	Class db.m5.xlarge		
Role Instance	Current activity  0 Sessions	Engine Oracle Enterprise Edition	Region & AZ -		
Connectivity & security		Monitoring	Logs & events	Configuration	Maintenance & backups
Tags					

Connecting to your sample Oracle DB instance

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to the DB instance. In this procedure, you connect to your sample DB instance by using the Oracle sqlplus command line utility. To download a standalone version of this utility, see [SQL*Plus User's Guide and Reference](#).

To connect to a DB instance using SQL*Plus

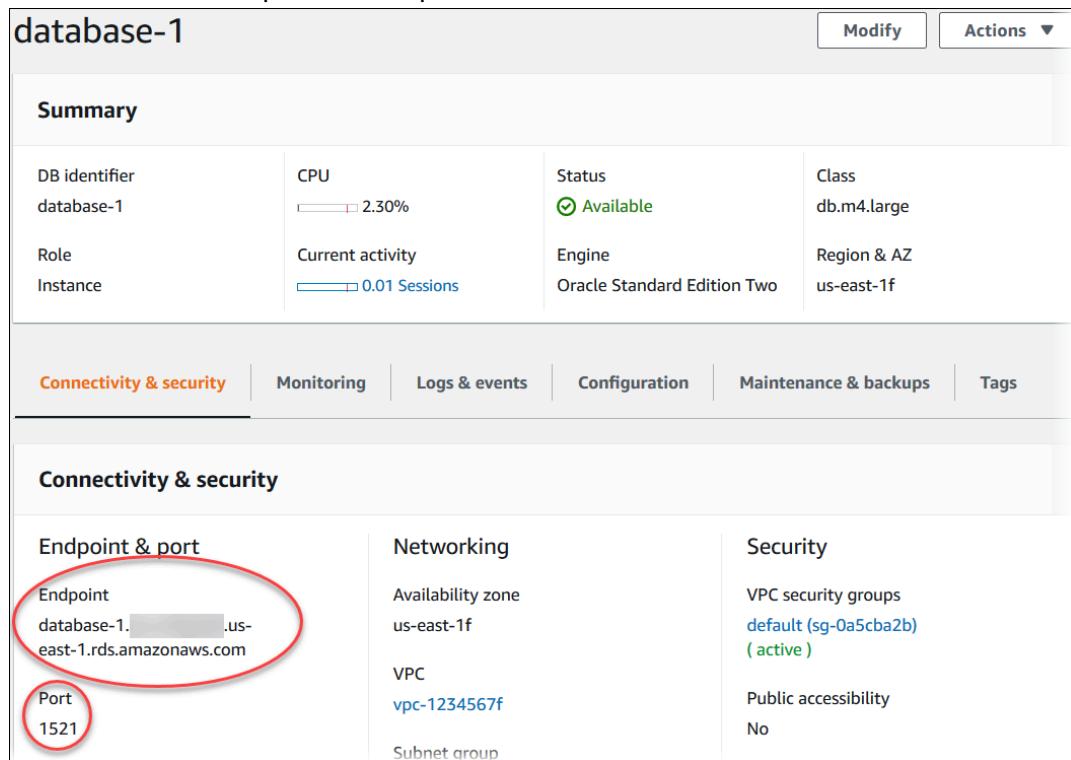
1. Make sure your DB instance is associated with a security group that provides access to it. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

If you didn't specify the appropriate security group when you created the DB instance, you can modify the DB instance to change its security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If your DB instance is publicly accessible, make sure its associated security group has inbound rules for the IP addresses that you want to access it. If your DB instance is private, make sure its associated security group has inbound rules for the security group of each resource to access it. An example is the security group for an Amazon EC2 instance.

2. Find the endpoint (DNS name) and port number for your DB instance.
 - a. Open the RDS console and then choose **Databases** to display a list of your DB instances.
 - b. Choose the Oracle DB instance name to display its details.
 - c. On the **Connectivity & security** tab, copy the following pieces of information:
 - Endpoint
 - Port

You need both the endpoint and the port number to connect to the DB instance.



Summary			
DB identifier	CPU	Status	Class
database-1	<div style="width: 20%;">2.30%</div>	Available	db.m4.large
Role	Current activity	Engine	Region & AZ
Instance	<div style="width: 10%;">0.01 Sessions</div>	Oracle Standard Edition Two	us-east-1f
Connectivity & security		Monitoring	Logs & events
Configuration		Maintenance & backups	Tags
Connectivity & security			
Endpoint & port Endpoint database-1...us-east-1.rds.amazonaws.com		Networking Availability zone us-east-1f	
Port 1521		Security VPC security groups default (sg-0a5cba2b) (active)	
		Public accessibility No	

- d. On the **Configuration** tab, copy the following pieces of information:

- DB name (not the DB instance ID)
- Master user name

You need both the DB name and the master user name to connect to the DB instance.

3. Enter the following command on one line at a command prompt to connect to your DB instance by using the sqlplus utility. Use the following values:
 - For **dbuser**, enter the name of the master user that you copied in the preceding steps.

- For HOST=*endpoint*, enter the endpoint that you copied in the preceding steps.
- For PORT=*portnum*, enter the port number that you copied in the preceding steps.
- For SID=*DB_NAME*, enter the Oracle database name (not the instance name) that you copied in the preceding steps.

```
sqlplus 'dbuser@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=endpoint)(PORT=portnum))(CONNECT_DATA=(SID=DB_NAME)))'
```

You should see output similar to the following.

```
SQL*Plus: Release 11.1.0.7.0 - Production on Wed May 25 15:13:59 2011  
SQL>
```

For more information about connecting to an Oracle DB instance, see [Connecting to your Oracle DB instance \(p. 1488\)](#). For information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Deleting your sample DB instance

After you explore the sample DB instance that you created, delete it so that you're no longer charged for it.

To delete a DB instance with no final DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to delete.
4. For **Actions**, choose **Delete**.
5. For **Create final snapshot?**, choose **No**, and choose the acknowledgment.
6. Choose **Delete**.

Creating a PostgreSQL DB instance and connecting to a database on a PostgreSQL DB instance

The easiest way to create a DB instance is to use the AWS Management Console. After you have created the DB instance, you can use standard SQL client utilities to connect to the DB instance, such as the pgAdmin utility. In this example, you create a DB instance running the PostgreSQL database engine called database-1, with a db.r6g.large DB instance class and 100 gibibytes (GiB) of storage.

Important

Before you can create or connect to a DB instance, make sure to complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

There's no charge for creating an AWS account. However, by completing this tutorial, you might incur costs for the AWS resources that you use. You can delete these resources after you complete the tutorial if they are no longer needed.

Contents

- [Creating a PostgreSQL DB instance \(p. 187\)](#)
- [Connecting to a PostgreSQL DB instance \(p. 191\)](#)
 - [Using pgAdmin to connect to a PostgreSQL DB instance \(p. 192\)](#)
 - [Using psql to connect to a PostgreSQL DB instance \(p. 197\)](#)
- [Deleting a DB instance \(p. 197\)](#)

Creating a PostgreSQL DB instance

The basic building block of Amazon RDS is the DB instance. This environment is where you run your PostgreSQL databases.

You can use **Easy create** to create a DB instance running PostgreSQL with the AWS Management Console. With **Easy create**, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default settings for the other configuration options. When you use **Standard create** instead of **Easy create**, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

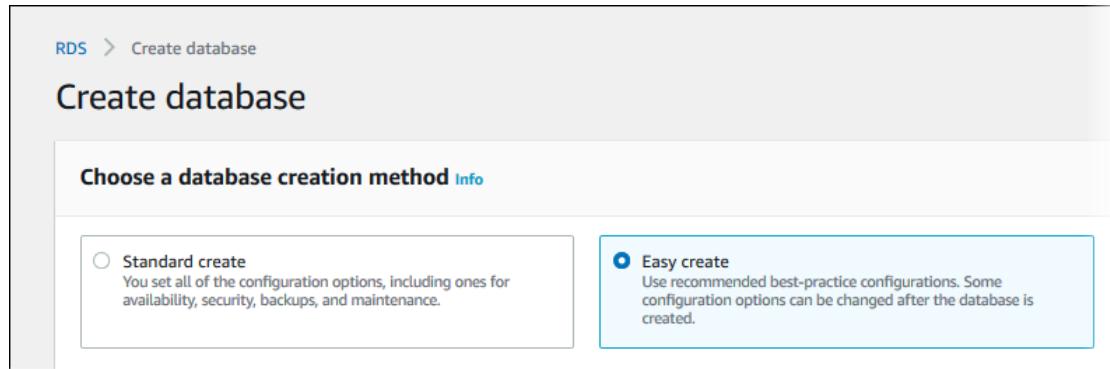
In this example, you use **Easy create** to create a DB instance running the PostgreSQL database engine with a db.r6g.large DB instance class.

Note

For information about creating DB instances with **Standard create**, see [Creating an Amazon RDS DB instance \(p. 230\)](#). If you want to use free tier, use **Standard create**.

To create a PostgreSQL DB instance with Easy create

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database** and make sure that **Easy create** is chosen.



5. In **Configuration**, choose **PostgreSQL**.
6. For **DB instance size**, choose **Dev/Test**.
7. For **DB instance identifier**, enter a name for the DB instance, or leave the default name.
8. For **Master username**, enter a name for the master user, or leave the default name (**postgres**).

The **Create database** page should look similar to the following image.

Create database

Choose a database creation method Info

Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Configuration

Engine type Info

Amazon Aurora



MySQL



MariaDB



PostgreSQL



Oracle



Microsoft SQL Server



DB instance size

Production

db.r6g.xlarge
4 vCPUs
32 GiB RAM
500 GiB

Dev/Test

db.r6g.large
2 vCPUs
16 GiB RAM
100 GiB

DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username Info

Type a login ID for the master user of your DB instance.

9. To use an automatically generated master password for the DB instance, make sure that the **Auto generate a password** box is selected.

To enter your master password, clear the **Auto generate a password** box, and then enter the same password in **Master password** and **Confirm password**.

10. (Optional) Open **View default settings for Easy create**.

▼ View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use [Standard Create](#).

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-2aed394c)	No
Option Group	default:postgres-13	No
Subnet Group	default	Yes
Automatic Backups	Enabled	Yes
VPC Security Group	sg-0b4ff871	Yes
Publically Accessible	No	Yes
Database Port	5432	Yes
DB Instance Identifier	database-1	Yes
DB Engine Version	13.3	Yes
DB Parameter Group	default.postgres13	Yes
Performance Insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto Minor Version Upgrade Enabled	Yes
Delete Protection	Not Enabled	Yes

You can examine the default settings used with **Easy create**. The **Editable after database is created** column shows which options you can change after database creation.

- To change settings with **No** in that column, use **Standard create**.
- To change settings with **Yes** in that column, either use **Standard create**, or modify the DB instance after it is created to change the settings.

The following are important considerations for changing the default settings:

- In some cases, you might want your DB instance to use a specific virtual private cloud (VPC) based on the Amazon VPC service. Or you might require a specific subnet group or security group. If so, use **Standard create** to specify these resources. You might have created these resources when you set up for Amazon RDS. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

- If you want to be able to access the DB instance from a client outside of its VPC, use **Standard create** to set **Public access** to **Yes**.

If the DB instance should be private, leave **Public access** set to **No**.

- If you want to use free tier, use **Standard create** to set the PostgreSQL version lower than version 13, and then choose **Free tier** in **Templates**.

11. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it.

If you need to change the master user password after the DB instance is available, you can modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

12. For **Databases**, choose the name of the new PostgreSQL DB instance.

On the RDS console, the details for new DB instance appear. The DB instance has a status of **Creating** until the DB instance is ready to use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new instance is available.

database-1				Modify	Actions ▾
Summary					
DB identifier	CPU	Status	Class		
database-1	-	Creating	db.r6g.large		
Role	Current activity	Engine	Region & AZ		
Instance	-1 Sessions	PostgreSQL	-		

[Connectivity & security](#) [Monitoring](#) [Logs & events](#) [Configuration](#) [Maintenance & backups](#)

Connecting to a PostgreSQL DB instance

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to the instance. Following, you can find two ways to connect to a PostgreSQL DB instance. The first example uses pgAdmin, a popular open-source administration and development tool for PostgreSQL. You can download and use pgAdmin without having a local instance of PostgreSQL on your client computer. The second example uses psql, a command line utility that is part of a PostgreSQL installation. To use psql, make sure that you have PostgreSQL or the psql client installed on your client computer.

Before you try connecting to the DB instance, make sure that the DB instance is associated with a security group that provides access to it. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

In some cases, you might have difficulty connecting to the DB instance. If so, the problem is most often with the access rules that you set up. These reside in the security group that you assigned to the DB instance. If you didn't specify the appropriate security group when you created the DB instance, you can modify the DB instance to change its security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If your DB instance is publicly accessible, make sure its associated security group has inbound rules for the IP addresses that you want to access it. If your DB instance is private, make sure its associated security group has inbound rules for the security group of each resource to access it. An example is the security group for an Amazon EC2 instance.

For more information about connecting to a PostgreSQL DB instance, see [Connecting to a DB instance running the PostgreSQL database engine \(p. 1809\)](#). If you can't connect to your DB instance, see [Troubleshooting connections to your RDS for PostgreSQL instance \(p. 1814\)](#).

Topics

- [Using pgAdmin to connect to a PostgreSQL DB instance \(p. 192\)](#)
- [Using psql to connect to a PostgreSQL DB instance \(p. 197\)](#)

Using pgAdmin to connect to a PostgreSQL DB instance

To connect to a PostgreSQL DB instance using pgAdmin

1. Find the endpoint (DNS name) and port number for your DB instance.
 - a. Open the RDS console and then choose **Databases** to display a list of your DB instances.
 - b. Choose the PostgreSQL DB instance name to display its details.
 - c. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the 'Summary' tab for a PostgreSQL DB instance named 'database-1'. The 'DB identifier' is listed as 'database-1'. Under the 'Role' section, 'Instance' is highlighted in orange. Below the summary, there are three tabs: 'Connectivity & security' (which is active and highlighted in red), 'Monitoring', and 'Logs & events'. The 'Connectivity & security' section displays the endpoint information. A red oval encircles the 'Endpoint' field ('database-1.us-west-1.rds.amazonaws.com') and the 'Port' field ('5432').

database-1

Summary

DB identifier
database-1

Role
Instance

Connectivity & security Monitoring Logs & events

Connectivity & security

Endpoint
database-1.us-west-1.rds.amazonaws.com

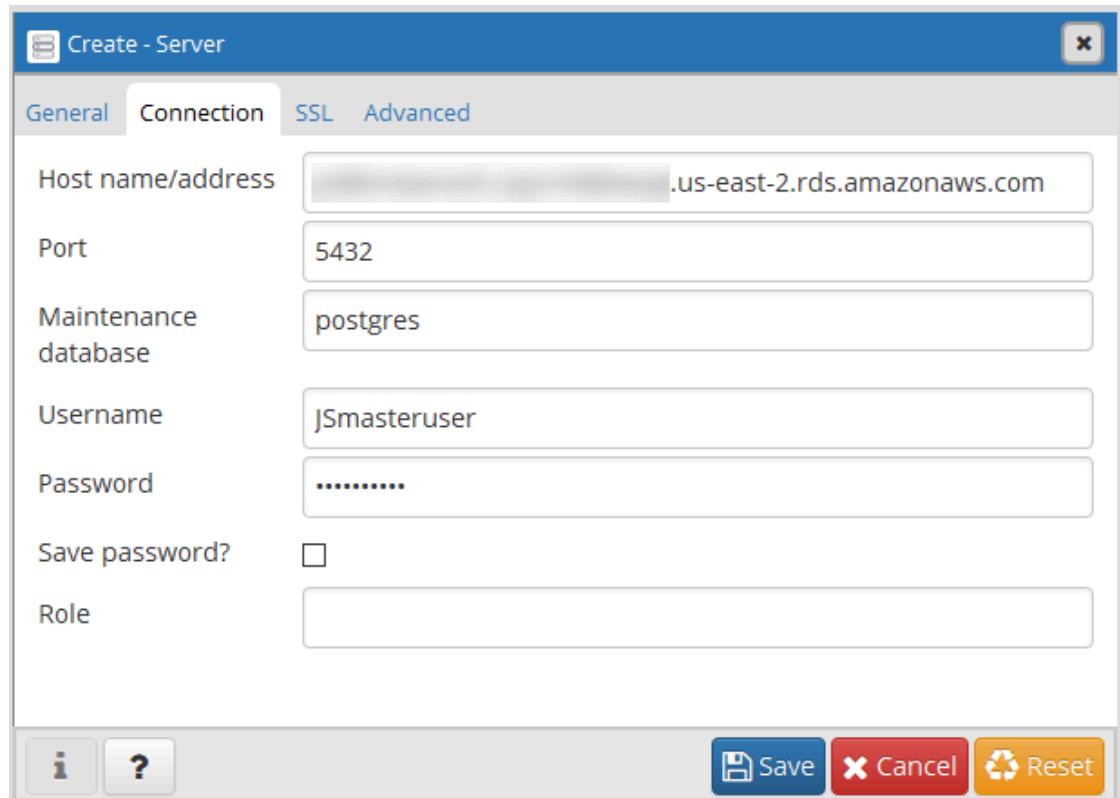
Port
5432

- d. On the **Configuration** tab, note the DB name. You don't need this to connect using pgAdmin, but you do need it to connect using psql.

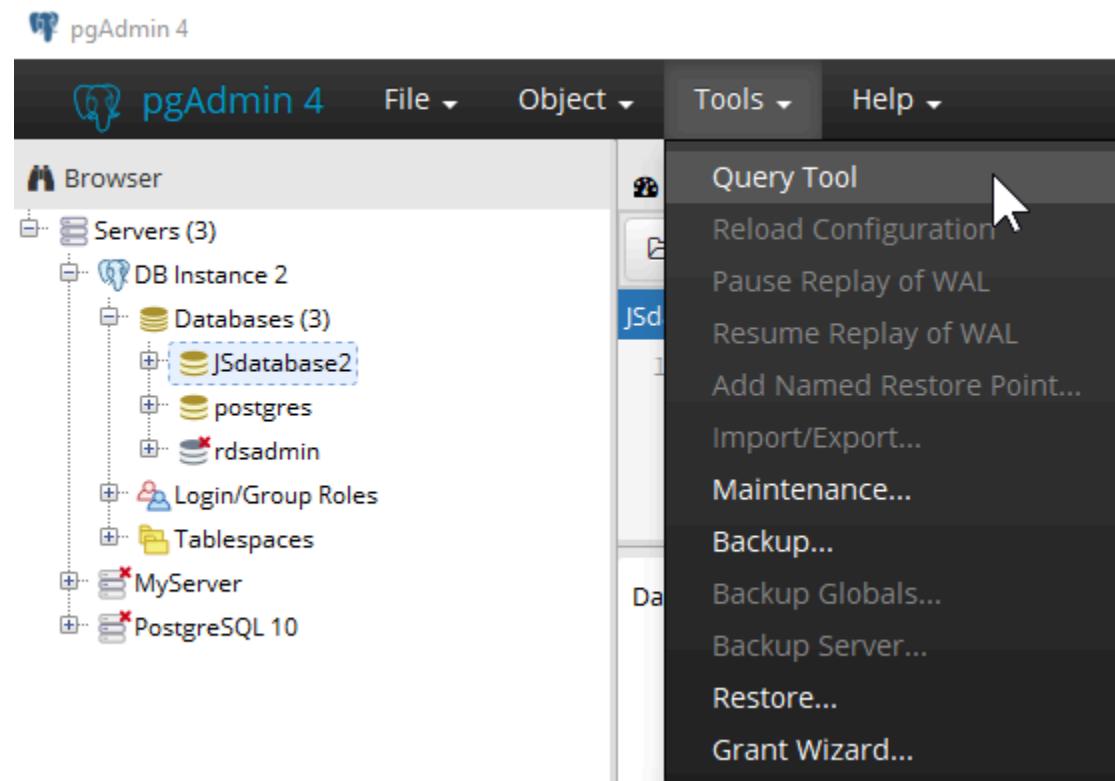
Connectivity & security	Monitoring	Logs & events	Configuration
Instance			
Configuration	Instance class	Storage	
DB instance ID	Instance class	Encryption	
database-1	db.m5.large	Enabled	
Engine version	vCPU	AWS KMS key	
13.4	2	aws/rds	
DB name	RAM	Storage type	
labdb	8 GB	General Purpose	

2. Install pgAdmin from <https://www.pgadmin.org/>. You can download and use pgAdmin without having a local instance of PostgreSQL on your client computer.
3. Launch the pgAdmin application on your client computer.
4. Choose **Add Server** from the **File** menu.
5. In the **New Server Registration** dialog box, enter the DB instance endpoint (for example, database-1.123456789012.us-west-1.rds.amazonaws.com) in the **Host** box. Don't include the colon or port number as shown on the Amazon RDS console (database-1.c6c8dntfzzhgv0.us-west-1.rds.amazonaws.com:5432).

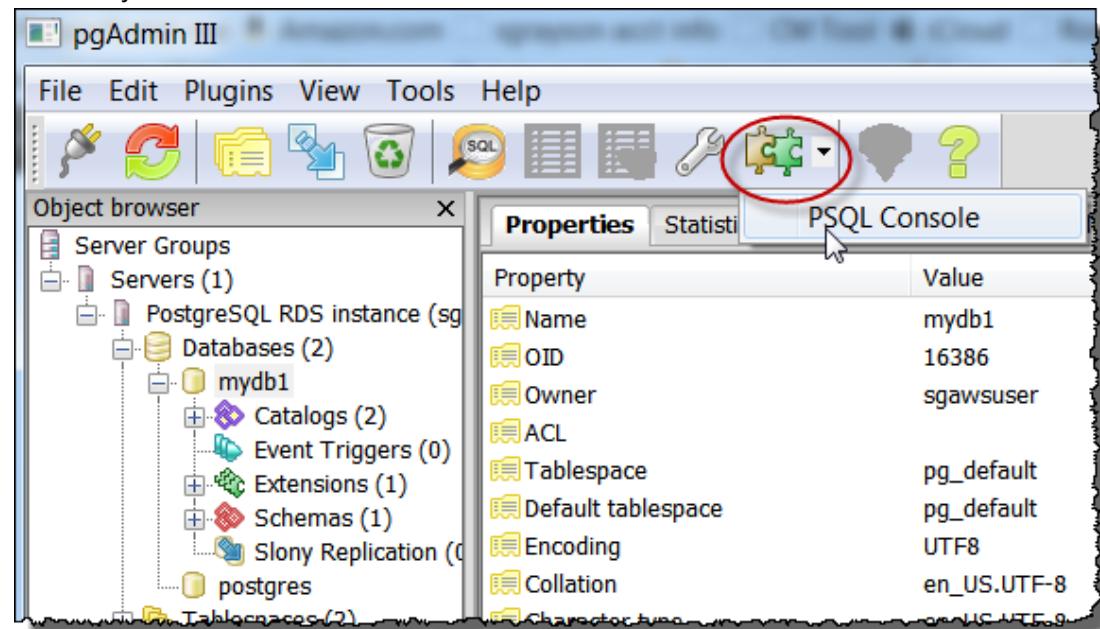
Enter the port you assigned to the DB instance for **Port**. Enter the user name and user password that you entered when you created the DB instance for **Username** and **Password**.



6. Choose **OK**.
7. In the Object browser, expand **Server Groups**. Choose the server (the DB instance) you created, and then choose the database name.



8. Choose the plugin icon and choose **PSQL Console**. The psql command window opens for the default database you created.



9. Use the command window to enter SQL or psql commands. Enter \q to close the window.

Using psql to connect to a PostgreSQL DB instance

If your client computer has PostgreSQL installed, you can use a local instance of psql to connect to a PostgreSQL DB instance. To connect to your PostgreSQL DB instance using psql, you provide host information, port number, access credentials, and the database name. You can obtain these details by following the first step in the procedure for [Using pgAdmin to connect to a PostgreSQL DB instance \(p. 192\)](#)

The following format is used to connect to a PostgreSQL DB instance on Amazon RDS.

```
psql --host=DB_instance_endpoint --port=port --username=master_user_name --password --  
dbname=database_name
```

For example, the following command connects to a database called mypgdb on a PostgreSQL DB instance called mypostgresql using fictitious credentials.

```
psql --host=database-1.123456789012.us-west-1.rds.amazonaws.com --port=5432 --  
username=awsuser --password --dbname=postgres
```

Deleting a DB instance

After you connect to the sample DB instance that you created, delete it so you're no longer charged for it.

To delete a DB instance with no final DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to delete.
4. For **Actions**, choose **Delete**.
5. For **Create final snapshot?**, choose **No**, and select the acknowledgment.
6. Choose **Delete**.

Tutorial: Create a web server and an Amazon RDS DB instance

This tutorial helps you install an Apache web server with PHP and create a MySQL database. The web server runs on an Amazon EC2 instance using Amazon Linux, and the MySQL database is a MySQL DB instance. Both the Amazon EC2 instance and the DB instance run in a virtual private cloud (VPC) based on the Amazon VPC service.

Important

There's no charge for creating an AWS account. However, by completing this tutorial, you might incur costs for the AWS resources you use. You can delete these resources after you complete the tutorial if they are no longer needed.

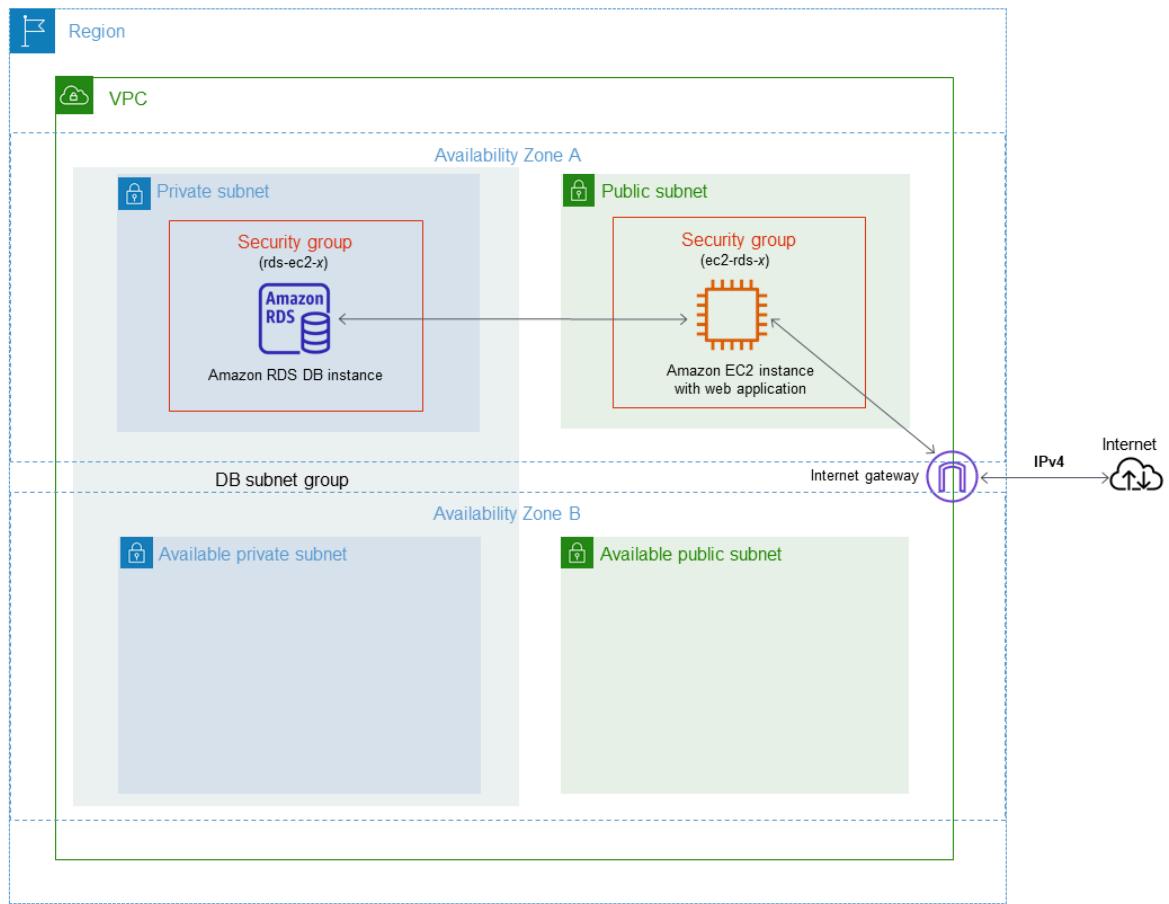
Note

This tutorial works with Amazon Linux and might not work for other versions of Linux such as Ubuntu.

In the tutorial that follows, you create an EC2 instance that uses the default VPC, subnets, and security group for your AWS account. This tutorial shows you how to create the DB instance and automatically set up connectivity with the EC2 instance that you created. The tutorial then shows you how to install the web server on the EC2 instance. You connect your web server to your DB instance in the VPC using the DB instance endpoint.

1. [Launch an EC2 instance \(p. 199\)](#)
2. [Create a DB instance \(p. 203\)](#)
3. [Install a web server on your EC2 instance \(p. 207\)](#)

The following diagram shows the configuration when the tutorial is complete.



Note

This tutorial uses the default VPC for your AWS account and automatically sets up connectivity between your EC2 instance and DB instance. If you would rather configure a new VPC for this scenario instead, complete the tasks in [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).

Launch an EC2 instance

Create an Amazon EC2 instance in the public subnet of your VPC.

To launch an EC2 instance

1. Sign in to the AWS Management Console and open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region where you want to create the EC2 instance.
3. Choose **EC2 Dashboard**, and then choose **Launch instance**, as shown following.

Resources

You are using the following Amazon EC2 resources in the US West (Oregon) Region:

Instances (running)	3	Dedicated Hosts	0
Instances	3	Key pairs	5
Placement groups	0	Security groups	10
Volumes	3		

i Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using [Learn more](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▾ [Migrate a server ↗](#)

Note: Your instances will launch in the US West (Oregon) Region

Service health

Region
US West (Oregon)

Zones

4. Make sure you have opted into the new launch experience.
5. Under **Name and tags**, for **Name**, enter **tutorial-ec2-instance-web-server**.
6. Under **Application and OS Images (Amazon Machine Image)**, choose **Amazon Linux**, and then choose the **Amazon Linux 2 AMI**. Keep the defaults for the other choices.

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents Quick Start

Amazon Linux Ubuntu Windows Red Hat SUSE Linux

aws ubuntu® Microsoft Red Hat SUSE

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type Free tier eligible

ami-098e42ae54c764c35 (64-bit (x86)) / ami-08e93a9522bbe6df6 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2 Kernel 5.10 AMI 2.0.20220606.1 x86_64 HVM gp2

Architecture AMI ID

64-bit (x86) ami-098e42ae54c764c35

7. Under **Instance type**, choose **t2.micro**.
8. Under **Key pair (login)**, choose a **Key pair name** to use an existing key pair. To create a new key pair for the Amazon EC2 instance, choose **Create new key pair** and then use the **Create key pair** window to create it.

For more information about creating a new key pair, see [Create a key pair](#) in the *Amazon EC2 User Guide for Linux Instances*.

9. Under **Network settings**, set these values and keep the other values as their defaults:
 - For **Allow SSH traffic from**, choose the source of SSH connections to the EC2 instance.

You can choose **My IP** if the displayed IP address is correct for SSH connections.

Otherwise, you can determine the IP address to use to connect to EC2 instances in your VPC using Secure Shell (SSH). To determine your public IP address, in a different browser window or tab, you can use the service at <https://checkip.amazonaws.com>. An example of an IP address is 203.0.113.25/32.

In many cases, you might connect through an internet service provider (ISP) or from behind your firewall without a static IP address. If so, make sure to determine the range of IP addresses used by client computers.

Warning

If you use `0.0.0.0/0` for SSH access, you make it possible for all IP addresses to access your public instances using SSH. This approach is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, authorize only a specific IP address or range of addresses to access your instances using SSH.

- Turn on **Allow HTTPs traffic from the internet**.
- Turn on **Allow HTTP traffic from the internet**.

▼ **Network settings** [Get guidance](#) [Edit](#)

Network [Info](#)
vpc-2aed394c

Subnet [Info](#)
No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)
Enable

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

[Create security group](#) [Select existing security group](#)

We'll create a new security group called '**launch-wizard-1**' with the following rules:

Allow SSH traffic from
Helps you connect to your instance My IP ▾

Allow HTTPs traffic from the internet
To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of `0.0.0.0/0` allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

10. Leave the default values for the remaining sections.
11. Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.
12. On the **Launch Status** page, shown following, note the identifier for your new EC2 instance, for example: `i-03a6ad47e97ba9dc5`.

The screenshot shows a success message: "Successfully initiated launch of instance (i-03a6ad47e97ba9dc5)". The instance ID is highlighted with a red oval. Below the message is a "Launch log" link.

Next Steps

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier)

How to connect to your instance
Your instance is launching and it might be a few minutes until it is in the running state, when it will be ready for you to use
Click View Instances to monitor your instance's status. Once your instance is in the 'running' state, you can connect to it from the Instances screen. Find out [how to connect to your instance](#)

[View more resources to get you started](#)

[View all instances](#)

13. Choose **View all instances** to find your instance.
14. Wait until **Instance state** for your instance is **Running** before continuing.
15. Complete [Create a DB instance \(p. 203\)](#).

Create a DB instance

Create an Amazon RDS for MySQL DB instance that maintains the data used by a web application.

To create a MySQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the AWS Management Console, check the AWS Region. It should be the same as the one where you created your EC2 instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.
5. On the **Create database** page, shown following, make sure that the **Standard create** option is chosen, and then choose **MySQL**.

RDS > Create database

Create database

Choose a database creation method [Info](#)

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

Amazon Aurora 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

Edition

MySQL Community

Known issues/limitations
Review the [Known issues/limitations](#) to learn about potential compatibility issues with specific database versions.

Version

6. In the **Templates** section, choose **Free tier**.
7. In the **Availability and durability** section, keep the defaults.
8. In the **Settings** section, set these values:
 - **DB instance identifier** – Type **tutorial-db-instance**.
 - **Master username** – Type **tutorial_user**.
 - **Auto generate a password** – Leave the option turned off.
 - **Master password** – Type a password.
 - **Confirm password** – Retype the password.

Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique cross all DB instances owned by your AWS account in the current AWS Region.

tutorial-db-instance

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Credentials Settings

Master username [Info](#)
Type a login ID for the master user of your DB instance.

tutorial_user

1 to 16 alphanumeric characters. First character must be a letter

Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

Confirm password [Info](#)

9. In the **Instance configuration** section, set these values:

- **Burstable classes (includes t classes)**
- **db.t3.micro**

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

Standard classes (includes m classes)
 Memory optimized classes (includes r and x classes)
 Burstable classes (includes t classes)

db.t3.micro
2 vCPUs 1 GiB RAM Network: 2,085 Mbps ▾

Include previous generation classes

10. In the **Storage** section, keep the defaults.

11. In the **Connectivity** section, set these values and keep the other values as their defaults:

- For **Compute resource**, choose **Connect to an EC2 compute resource**.
- For **EC2 instance**, choose the EC2 instance you created previously, such as **tutorial-ec2-instance-web-server**.

The screenshot shows the 'Connectivity' configuration section. It includes two radio button options: 'Don't connect to an EC2 compute resource' (unchecked) and 'Connect to an EC2 compute resource' (checked). A note below explains that selecting 'Connect to an EC2 compute resource' will automatically set up connectivity settings. Below this is the 'EC2 Instance' section, which lists the selected EC2 instance as 'tutorial-ec2-instance-web-server'. A callout box provides a note about VPC settings.

Connectivity Info

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

EC2 Instance Info
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

tutorial-ec2-instance-web-server ▾

i Some VPC settings can't be changed when a compute resource is added
Adding an EC2 compute resource automatically selects the VPC, DB subnet group, and public access settings for this database. To allow the EC2 instance to access the database, a VPC security group rds-ec2-X is added to the database and another called ec2-rds-X to the EC2 instance. You can remove the new security group for the database only by removing the compute resource.

12. In the **Database authentication** section, make sure **Password authentication** is selected.
13. Open the **Additional configuration** section, and enter **sample** for **Initial database name**. Keep the default settings for the other options.
14. To create your MySQL DB instance, choose **Create database**.

Your new DB instance appears in the **Databases** list with the status **Creating**.

15. Wait for the **Status** of your new DB instance to show as **Available**. Then choose the DB instance name to show its details.
16. In the **Connectivity & security** section, view the **Endpoint** and **Port** of the DB instance.

RDS > Databases > tutorial-db-instance

tutorial-db-instance

Summary

DB identifier	tutorial-db-instance	CPU	3.10%
Role	Instance	Current activity	0 Connections

Connectivity & security Monitoring Logs & events Configuration Maintenance

Connectivity & security

Endpoint & port	Networking
Endpoint	Availability Zone
tutorial-db-instance.[REDACTED].west-2.rds.amazonaws.com	us-west-2a
Port	VPC
3306	tutorial-vpc (vpc-04badc20a546242e6)
	Subnet group

Note the endpoint and port for your DB instance. You use this information to connect your web server to your DB instance.

17. Complete [Install a web server on your EC2 instance \(p. 207\)](#).

Install a web server on your EC2 instance

Install a web server on the EC2 instance you created in [Launch an EC2 instance \(p. 199\)](#). The web server connects to the Amazon RDS DB instance that you created in [Create a DB instance \(p. 203\)](#).

Install an Apache web server with PHP and MariaDB

Connect to your EC2 instance and install the web server.

To connect to your EC2 instance and install the Apache web server with PHP

1. Connect to the EC2 instance that you created earlier by following the steps in [Connect to your Linux instance](#).
2. Get the latest bug fixes and security updates by updating the software on your EC2 instance. To do this, use the following command.

Note

The `-y` option installs the updates without asking for confirmation. To examine updates before installing, omit this option.

```
sudo yum update -y
```

3. After the updates complete, install the PHP software using the `amazon-linux-extras install` command. This command installs multiple software packages and related dependencies at the same time.

```
sudo amazon-linux-extras install php8.0 mariadb10.5
```

If you receive an error stating `sudo: amazon-linux-extras: command not found`, your instance wasn't launched with an Amazon Linux 2 AMI. You might be using the Amazon Linux AMI instead. You can view your version of Amazon Linux using the following command.

```
cat /etc/system-release
```

For more information, see [Updating instance software](#).

4. Install the Apache web server.

```
sudo yum install -y httpd
```

5. Start the web server with the command shown following.

```
sudo systemctl start httpd
```

You can test that your web server is properly installed and started. To do this, enter the public Domain Name System (DNS) name of your EC2 instance in the address bar of a web browser, for example: `http://ec2-42-8-168-21.us-west-1.compute.amazonaws.com`. If your web server is running, then you see the Apache test page.

If you don't see the Apache test page, check your inbound rules for the VPC security group that you created in [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#). Make sure that your inbound rules include one allowing HTTP (port 80) access for the IP address to connect to the web server.

Note

The Apache test page appears only when there is no content in the document root directory, `/var/www/html`. After you add content to the document root directory, your content appears at the public DNS address of your EC2 instance. Before this point, it appears on the Apache test page.

6. Configure the web server to start with each system boot using the `systemctl` command.

```
sudo systemctl enable httpd
```

To allow ec2-user to manage files in the default root directory for your Apache web server, modify the ownership and permissions of the /var/www directory. There are many ways to accomplish this task. In this tutorial, you add ec2-user to the apache group, to give the apache group ownership of the /var/www directory and assign write permissions to the group.

To set file permissions for the Apache web server

1. Add the ec2-user user to the apache group.

```
sudo usermod -a -G apache ec2-user
```

2. Log out to refresh your permissions and include the new apache group.

```
exit
```

3. Log back in again and verify that the apache group exists with the groups command.

```
groups
```

Your output looks similar to the following:

```
ec2-user adm wheel apache systemd-journal
```

4. Change the group ownership of the /var/www directory and its contents to the apache group.

```
sudo chown -R ec2-user:apache /var/www
```

5. Change the directory permissions of /var/www and its subdirectories to add group write permissions and set the group ID on subdirectories created in the future.

```
sudo chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} \;
```

6. Recursively change the permissions for files in the /var/www directory and its subdirectories to add group write permissions.

```
find /var/www -type f -exec sudo chmod 0664 {} \;
```

Now, ec2-user (and any future members of the apache group) can add, delete, and edit files in the Apache document root. This makes it possible for you to add content, such as a static website or a PHP application.

Note

A web server running the HTTP protocol provides no transport security for the data that it sends or receives. When you connect to an HTTP server using a web browser, much information is visible to eavesdroppers anywhere along the network pathway. This information includes the URLs that you visit, the content of webpages that you receive, and the contents (including passwords) of any HTML forms.

The best practice for securing your web server is to install support for HTTPS (HTTP Secure). This protocol protects your data with SSL/TLS encryption. For more information, see [Tutorial: Configure SSL/TLS with the Amazon Linux AMI](#) in the *Amazon EC2 User Guide*.

Connect your Apache web server to your DB instance

Next, you add content to your Apache web server that connects to your Amazon RDS DB instance.

To add content to the Apache web server that connects to your DB instance

1. While still connected to your EC2 instance, change the directory to /var/www and create a new subdirectory named inc.

```
cd /var/www
mkdir inc
cd inc
```

2. Create a new file in the inc directory named dbinfo.inc, and then edit the file by calling nano (or the editor of your choice).

```
>dbinfo.inc
nano dbinfo.inc
```

3. Add the following contents to the dbinfo.inc file. Here, *db_instance_endpoint* is your DB instance endpoint, without the port, and *master password* is the master password for your DB instance.

Note

We recommend placing the user name and password information in a folder that isn't part of the document root for your web server. Doing this reduces the possibility of your security information being exposed.

```
<?php

define('DB_SERVER', 'db_instance_endpoint');
define('DB_USERNAME', 'tutorial_user');
define('DB_PASSWORD', 'master password');
define('DB_DATABASE', 'sample');

?>
```

4. Save and close the dbinfo.inc file.
5. Change the directory to /var/www/html.

```
cd /var/www/html
```

6. Create a new file in the html directory named SamplePage.php, and then edit the file by calling nano (or the editor of your choice).

```
>SamplePage.php
nano SamplePage.php
```

7. Add the following contents to the SamplePage.php file:

```
<?php include "../inc/dbinfo.inc"; ?>
<html>
<body>
<h1>Sample page</h1>
<?php

/* Connect to MySQL and select the database. */
$connection = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD);

if (mysqli_connect_errno()) echo "Failed to connect to MySQL: " .
mysqli_connect_error();
```

```

$database = mysqli_select_db($connection, DB_DATABASE);

/* Ensure that the EMPLOYEES table exists. */
VerifyEmployeesTable($connection, DB_DATABASE);

/* If input fields are populated, add a row to the EMPLOYEES table. */
$employee_name = htmlentities($_POST['NAME']);
$employee_address = htmlentities($_POST['ADDRESS']);

if (strlen($employee_name) || strlen($employee_address)) {
    AddEmployee($connection, $employee_name, $employee_address);
}
?>

<!-- Input form -->
<form action=<?PHP echo $_SERVER['SCRIPT_NAME'] ?>" method="POST">
    <table border="0">
        <tr>
            <td>NAME</td>
            <td>ADDRESS</td>
        </tr>
        <tr>
            <td>
                <input type="text" name="NAME" maxlength="45" size="30" />
            </td>
            <td>
                <input type="text" name="ADDRESS" maxlength="90" size="60" />
            </td>
            <td>
                <input type="submit" value="Add Data" />
            </td>
        </tr>
    </table>
</form>

<!-- Display table data. -->
<table border="1" cellpadding="2" cellspacing="2">
    <tr>
        <td>ID</td>
        <td>NAME</td>
        <td>ADDRESS</td>
    </tr>
?>

<?php

$result = mysqli_query($connection, "SELECT * FROM EMPLOYEES");

while($query_data = mysqli_fetch_row($result)) {
    echo "<tr>";
    echo "<td>",$query_data[0], "</td>",
          "<td>",$query_data[1], "</td>",
          "<td>",$query_data[2], "</td>";
    echo "</tr>";
}
?>

</table>

<!-- Clean up. -->
<?php

    mysqli_free_result($result);
    mysqli_close($connection);

?>

```

```

</body>
</html>

<?php

/* Add an employee to the table. */
function AddEmployee($connection, $name, $address) {
    $n = mysqli_real_escape_string($connection, $name);
    $a = mysqli_real_escape_string($connection, $address);

    $query = "INSERT INTO EMPLOYEES (NAME, ADDRESS) VALUES ('$n', '$a');";

    if(!mysqli_query($connection, $query)) echo("<p>Error adding employee data.</p>");

}

/* Check whether the table exists and, if not, create it. */
function VerifyEmployeesTable($connection, $dbName) {
    if(!TableExists("EMPLOYEES", $connection, $dbName))
    {
        $query = "CREATE TABLE EMPLOYEES (
            ID int(11) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
            NAME VARCHAR(45),
            ADDRESS VARCHAR(90)
        )";

        if(!mysqli_query($connection, $query)) echo("<p>Error creating table.</p>");

    }
}

/* Check for the existence of a table. */
function TableExists($tableName, $connection, $dbName) {
    $t = mysqli_real_escape_string($connection, $tableName);
    $d = mysqli_real_escape_string($connection, $dbName);

    $checktable = mysqli_query($connection,
        "SELECT TABLE_NAME FROM information_schema.TABLES WHERE TABLE_NAME = '$t' AND
        TABLE_SCHEMA = '$d'");

    if(mysqli_num_rows($checktable) > 0) return true;

    return false;
}
?>
```

8. Save and close the SamplePage.php file.
9. Verify that your web server successfully connects to your DB instance by opening a web browser and browsing to <http://EC2 instance endpoint>/SamplePage.php, for example: <http://ec2-55-122-41-31.us-west-2.compute.amazonaws.com>/SamplePage.php.

You can use SamplePage.php to add data to your DB instance. The data that you add is then displayed on the page. To verify that the data was inserted into the table, install MySQL client on the Amazon EC2 instance. Then connect to the DB instance and query the table.

For information about installing the MySQL client and connecting to a DB instance, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#).

To make sure that your DB instance is as secure as possible, verify that sources outside of the VPC can't connect to your DB instance.

After you have finished testing your web server and your database, you should delete your DB instance and your Amazon EC2 instance.

- To delete a DB instance, follow the instructions in [Deleting a DB instance \(p. 421\)](#). You don't need to create a final snapshot.
- To terminate an Amazon EC2 instance, follow the instruction in [Terminate your instance](#) in the *Amazon EC2 User Guide*.

Amazon RDS tutorials and sample code

The AWS documentation includes several tutorials that guide you through common Amazon RDS use cases. Many of these tutorials show you how to use Amazon RDS with other AWS services. In addition, you can access sample code in GitHub.

Note

You can find more tutorials at the [AWS Database Blog](#). For information about training, see [AWS Training and Certification](#).

Topics

- [Tutorials in this guide \(p. 214\)](#)
- [Tutorials in other AWS guides \(p. 215\)](#)
- [Tutorials and sample code in GitHub \(p. 215\)](#)

Tutorials in this guide

The following tutorials in this guide show you how to perform common tasks with Amazon RDS:

- [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#)

Learn how to include a DB instance in a virtual private cloud (VPC) based on the Amazon VPC service. In this case, the VPC shares data with a web server that is running on an Amazon EC2 instance in the same VPC.

- [Tutorial: Create a VPC for use with a DB instance \(dual-stack mode\) \(p. 2126\)](#)

Learn how to include a DB instance in a virtual private cloud (VPC) based on the Amazon VPC service. In this case, the VPC shares data with an Amazon EC2 instance in the same VPC. In this tutorial, you create the VPC for this scenario that works with a database running in dual-stack mode.

- [Tutorial: Create a web server and an Amazon RDS DB instance \(p. 198\)](#)

Learn how to install an Apache web server with PHP and create a MySQL database. The web server runs on an Amazon EC2 instance using Amazon Linux, and the MySQL database is a MySQL DB instance. Both the Amazon EC2 instance and the DB instance run in an Amazon VPC.

- [Tutorial: Restore an Amazon RDS DB instance from a DB snapshot \(p. 507\)](#)

Learn how to restore a DB instance from a DB snapshot.

- [Tutorial: Use tags to specify which DB instances to stop \(p. 397\)](#)

Learn how to use tags to specify which DB instances to stop.

- [Tutorial: Log DB instance state changes using Amazon EventBridge \(p. 665\)](#)

Learn how to log a DB instance state change using Amazon EventBridge and AWS Lambda.

- [Tutorial: Creating an Amazon CloudWatch alarm for Multi-AZ DB cluster replica lag \(p. 536\)](#)

Learn how to create a CloudWatch alarm that sends an Amazon SNS message when replica lag for a Multi-AZ DB cluster has exceeded a threshold. An alarm watches the ReplicaLag metric over a time

period that you specify. The action is a notification sent to an Amazon SNS topic or Amazon EC2 Auto Scaling policy.

Tutorials in other AWS guides

The following tutorials in other AWS guides show you how to perform common tasks with Amazon RDS:

- [Tutorial: Rotating a Secret for an AWS Database](#) in the *AWS Secrets Manager User Guide*
Learn how to create a secret for an AWS database and configure the secret to rotate on a schedule. You trigger one rotation manually, and then confirm that the new version of the secret continues to provide access.
- [Tutorial: Configuring a Lambda function to access Amazon RDS in an Amazon VPC](#) in the *AWS Lambda Developer Guide*
Learn how to create a Lambda function to access a database, create a table, add a few records, and retrieve the records from the table. You also learn how to invoke the Lambda function and verify the query results.
- [Tutorials and samples](#) in the *AWS Elastic Beanstalk Developer Guide*
Learn how to deploy applications that use Amazon RDS databases with AWS Elastic Beanstalk.
- [Using Data from an Amazon RDS Database to Create an Amazon ML Datasource](#) in the *Amazon Machine Learning Developer Guide*
Learn how to create an Amazon Machine Learning (Amazon ML) datasource object from data stored in a MySQL DB instance.
- [Manually Enabling Access to an Amazon RDS Instance in a VPC](#) in the *Amazon QuickSight User Guide*
Learn how to enable Amazon QuickSight access to an Amazon RDS DB instance in a VPC.

Tutorials and sample code in GitHub

The following tutorials and sample code in GitHub show you how to perform common tasks with Amazon RDS:

- [Creating the Amazon Relational Database Service item tracker](#)
Learn how to create an application that tracks and reports on work items. This application uses Amazon RDS, Amazon Simple Email Service, Elastic Beanstalk, and SDK for Java 2.x.
- [SDK for Go code examples for Amazon RDS](#)
View a collection of SDK for Go code examples for Amazon RDS and Aurora.
- [SDK for Java 2.x code examples for Amazon RDS](#)
View a collection of SDK for Java 2.x code examples for Amazon RDS and Aurora.
- [SDK for PHP code examples for Amazon RDS](#)
View a collection of SDK for PHP code examples for Amazon RDS and Aurora.
- [SDK for Ruby code examples for Amazon RDS](#)
View a collection of SDK for Ruby code examples for Amazon RDS and Aurora.

Best practices for Amazon RDS

Learn best practices for working with Amazon RDS. As new best practices are identified, we will keep this section up to date.

Topics

- [Amazon RDS basic operational guidelines \(p. 216\)](#)
- [DB instance RAM recommendations \(p. 217\)](#)
- [Using Enhanced Monitoring to identify operating system issues \(p. 217\)](#)
- [Using metrics to identify performance issues \(p. 217\)](#)
- [Tuning queries \(p. 221\)](#)
- [Best practices for working with MySQL \(p. 222\)](#)
- [Best practices for working with MariaDB \(p. 223\)](#)
- [Best practices for working with Oracle \(p. 224\)](#)
- [Best practices for working with PostgreSQL \(p. 224\)](#)
- [Best practices for working with SQL Server \(p. 226\)](#)
- [Working with DB parameter groups \(p. 227\)](#)
- [Best practices for automating DB instance creation \(p. 227\)](#)
- [Amazon RDS new features and best practices presentation video \(p. 228\)](#)

Note

For common recommendations for Amazon RDS, see [Viewing Amazon RDS recommendations \(p. 520\)](#).

Amazon RDS basic operational guidelines

The following are basic operational guidelines that everyone should follow when working with Amazon RDS. Note that the Amazon RDS Service Level Agreement requires that you follow these guidelines:

- Use metrics to monitor your memory, CPU, replica lag, and storage usage. You can set up Amazon CloudWatch to notify you when usage patterns change or when you approach the capacity of your deployment. This way, you can maintain system performance and availability.
- Scale up your DB instance when you are approaching storage capacity limits. You should have some buffer in storage and memory to accommodate unforeseen increases in demand from your applications.
- Enable automatic backups and set the backup window to occur during the daily low in write IOPS. That's when a backup is least disruptive to your database usage.
- If your database workload requires more I/O than you have provisioned, recovery after a failover or database failure will be slow. To increase the I/O capacity of a DB instance, do any or all of the following:
 - Migrate to a different DB instance class with high I/O capacity.
 - Convert from magnetic storage to either General Purpose or Provisioned IOPS storage, depending on how much of an increase you need. For information on available storage types, see [Amazon RDS storage types \(p. 64\)](#).

If you convert to Provisioned IOPS storage, make sure you also use a DB instance class that is optimized for Provisioned IOPS. For information on Provisioned IOPS, see [Provisioned IOPS SSD storage \(p. 66\)](#).

- If you are already using Provisioned IOPS storage, provision additional throughput capacity.
- If your client application is caching the Domain Name Service (DNS) data of your DB instances, set a time-to-live (TTL) value of less than 30 seconds. The underlying IP address of a DB instance can change after a failover. Caching the DNS data for an extended time can thus lead to connection failures. Your application might try to connect to an IP address that's no longer in service.
- Test failover for your DB instance to understand how long the process takes for your particular use case. Also test failover to ensure that the application that accesses your DB instance can automatically connect to the new DB instance after failover occurs.

DB instance RAM recommendations

An Amazon RDS performance best practice is to allocate enough RAM so that your *working set* resides almost completely in memory. The working set is the data and indexes that are frequently in use on your instance. The more you use the DB instance, the more the working set will grow.

To tell if your working set is almost all in memory, check the ReadIOPS metric (using Amazon CloudWatch) while the DB instance is under load. The value of ReadIOPS should be small and stable. In some cases, scaling up the DB instance class to a class with more RAM results in a dramatic drop in ReadIOPS. In these cases, your working set was not almost completely in memory. Continue to scale up until ReadIOPS no longer drops dramatically after a scaling operation, or ReadIOPS is reduced to a very small amount. For information on monitoring a DB instance's metrics, see [Viewing metrics in the Amazon RDS console \(p. 525\)](#).

Using Enhanced Monitoring to identify operating system issues

When Enhanced Monitoring is enabled, Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console. You can also consume the Enhanced Monitoring JSON output from Amazon CloudWatch Logs in a monitoring system of your choice. For more information about Enhanced Monitoring, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

Using metrics to identify performance issues

To identify performance issues caused by insufficient resources and other common bottlenecks, you can monitor the metrics available for your Amazon RDS DB instance.

Viewing performance metrics

You should monitor performance metrics on a regular basis to see the average, maximum, and minimum values for a variety of time ranges. If you do so, you can identify when performance is degraded. You can also set Amazon CloudWatch alarms for particular metric thresholds so you are alerted if they are reached.

To troubleshoot performance issues, it's important to understand the baseline performance of the system. When you set up a DB instance and run it with a typical workload, capture the average, maximum, and minimum values of all performance metrics. Do so at a number of different intervals (for example, one hour, 24 hours, one week, two weeks). This can give you an idea of what is normal. It helps to get comparisons for both peak and off-peak hours of operation. You can then use this information to identify when performance is dropping below standard levels.

If you use Multi-AZ DB clusters, monitor the time difference between the latest transaction on the writer DB instance and the latest applied transaction on a reader DB instance. This difference is called *replica lag*. For more information, see [Replica lag and Multi-AZ DB clusters \(p. 133\)](#).

To view performance metrics

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose a DB instance.
3. Choose **Monitoring**. The first eight performance metrics display. The metrics default to showing information for the current day.
4. Use the numbered buttons at top right to page through the additional metrics, or adjust the settings to see more metrics.
5. Choose a performance metric to adjust the time range in order to see data for other than the current day. You can change the **Statistic**, **Time Range**, and **Period** values to adjust the information displayed. For example, you might want to see the peak values for a metric for each day of the last two weeks. If so, set **Statistic** to **Maximum**, **Time Range** to **Last 2 Weeks**, and **Period** to **Day**.

Note

Changing the **Statistic**, **Time Range**, and **Period** values changes them for all metrics. The updated values persist for the remainder of your session or until you change them again.

You can also view performance metrics using the CLI or API. For more information, see [Viewing metrics in the Amazon RDS console \(p. 525\)](#).

To set a CloudWatch alarm

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose a DB instance.
3. Choose **Logs & events**.
4. In the **CloudWatch alarms** section, choose **Create alarm**.

Create alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

Settings

[Refresh](#)

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send notifications

- Yes
 No

Send notifications to

- ARN
 New email or SMS topic

Topic name

Name of the topic.

Manually enter a topic name...

With these recipients

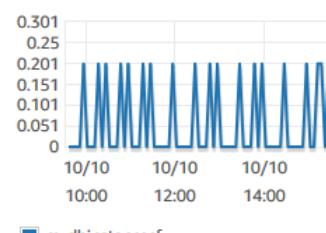
Email addresses or phone numbers of SMS enabled devices to send the notifications to

awsAccount@domain.com

Metric

Average ▼ of CPU Utilization ▼

CPU Utilization Percent



Threshold

>= ▼ ▲ Percent

Evaluation period

1 ▲ consecutive period(s) of 5 Minutes ▼

Name of alarm

awsrds-mydbinstancecf-High-CPU-Utilization

[Cancel](#)

[Create alarm](#)

5. For **Send notifications**, choose **Yes**, and for **Send notifications to**, choose **New email or SMS topic**.
6. For **Topic name**, enter a name for the notification, and for **With these recipients**, enter a comma-separated list of email addresses and phone numbers.
7. For **Metric**, choose the alarm statistic and metric to set.
8. For **Threshold**, specify whether the metric must be greater than, less than, or equal to the threshold, and specify the threshold value.
9. For **Evaluation period**, choose the evaluation period for the alarm. For **consecutive period(s) of**, choose the period during which the threshold must have been reached in order to trigger the alarm.
10. For **Name of alarm**, enter a name for the alarm.
11. Choose **Create Alarm**.

The alarm appears in the **CloudWatch alarms** section.

Evaluating performance metrics

A DB instance has a number of different categories of metrics, and how to determine acceptable values depends on the metric.

CPU

- CPU Utilization – Percentage of computer processing capacity used.

Memory

- Freeable Memory – How much RAM is available on the DB instance, in megabytes. The red line in the Monitoring tab metrics is marked at 75% for CPU, Memory and Storage Metrics. If instance memory consumption frequently crosses that line, then this indicates that you should check your workload or upgrade your instance.
- Swap Usage – How much swap space is used by the DB instance, in megabytes.

Disk space

- Free Storage Space – How much disk space is not currently being used by the DB instance, in megabytes.

Input/output operations

- Read IOPS, Write IOPS – The average number of disk read or write operations per second.
- Read Latency, Write Latency – The average time for a read or write operation in milliseconds.
- Read Throughput, Write Throughput – The average number of megabytes read from or written to disk per second.
- Queue Depth – The number of I/O operations that are waiting to be written to or read from disk.

Network traffic

- Network Receive Throughput, Network Transmit Throughput – The rate of network traffic to and from the DB instance in bytes per second.

Database connections

- DB Connections – The number of client sessions that are connected to the DB instance.

For more detailed individual descriptions of the performance metrics available, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).

Generally speaking, acceptable values for performance metrics depend on what your baseline looks like and what your application is doing. Investigate consistent or trending variances from your baseline. Advice about specific types of metrics follows:

- **High CPU or RAM consumption** – High values for CPU or RAM consumption might be appropriate. For example, they might be so if they are in keeping with your goals for your application (like throughput or concurrency) and are expected.

- **Disk space consumption** – Investigate disk space consumption if space used is consistently at or above 85 percent of the total disk space. See if it is possible to delete data from the instance or archive data to a different system to free up space.
- **Network traffic** – For network traffic, talk with your system administrator to understand what expected throughput is for your domain network and internet connection. Investigate network traffic if throughput is consistently lower than expected.
- **Database connections** – Consider constraining database connections if you see high numbers of user connections in conjunction with decreases in instance performance and response time. The best number of user connections for your DB instance will vary based on your instance class and the complexity of the operations being performed. To determine the number of database connections, associate your DB instance with a parameter group. In this group, set the *User Connections* parameter to other than 0 (unlimited). You can either use an existing parameter group or create a new one. For more information, see [Working with parameter groups \(p. 289\)](#).
- **IOPS metrics** – The expected values for IOPS metrics depend on disk specification and server configuration, so use your baseline to know what is typical. Investigate if values are consistently different than your baseline. For best IOPS performance, make sure your typical working set will fit into memory to minimize read and write operations.

For issues with performance metrics, a first step to improve performance is to tune the most used and most expensive queries. Tune them to see if doing so lowers the pressure on system resources. For more information, see [Tuning queries \(p. 221\)](#).

If your queries are tuned and an issue persists, consider upgrading your Amazon RDS [DB instance classes \(p. 10\)](#). You might upgrade it to one with more of the resource (CPU, RAM, disk space, network bandwidth, I/O capacity) that is related to the issue.

Tuning queries

One of the best ways to improve DB instance performance is to tune your most commonly used and most resource-intensive queries. Here, you tune them to make them less expensive to run. For information on improving queries, use the following resources:

- MySQL – See [Optimizing SELECT statements](#) in the MySQL documentation. For additional query tuning resources, see [MySQL performance tuning and optimization resources](#).
- Oracle – See [Database SQL Tuning Guide](#) in the Oracle Database documentation.
- SQL Server – See [Analyzing a query](#) in the Microsoft documentation. You can also use the execution-, index-, and I/O-related data management views (DMVs) described in [System Dynamic Management Views](#) in the Microsoft documentation to troubleshoot SQL Server query issues.

A common aspect of query tuning is creating effective indexes. For potential index improvements for your DB instance, see [Database Engine Tuning Advisor](#) in the Microsoft documentation. For information on using Tuning Advisor on RDS for SQL Server, see [Analyzing your database workload on an Amazon RDS for SQL Server DB instance with Database Engine Tuning Advisor \(p. 1294\)](#).

- PostgreSQL – See [Using EXPLAIN](#) in the PostgreSQL documentation to learn how to analyze a query plan. You can use this information to modify a query or underlying tables in order to improve query performance.

For information about how to specify joins in your query for the best performance, see [Controlling the planner with explicit JOIN clauses](#).

- MariaDB – See [Query optimizations](#) in the MariaDB documentation.

Best practices for working with MySQL

Both table sizes and number of tables in a MySQL database can affect performance.

Table size

Typically, operating system constraints on file sizes determine the effective maximum table size for MySQL databases. So, the limits usually aren't determined by internal MySQL constraints.

On a MySQL DB instance, avoid tables in your database growing too large. Although the general storage limit is 64 TiB, provisioned storage limits restrict the maximum size of a MySQL table file to 16 TiB. Partition your large tables so that file sizes are well under the 16 TiB limit. This approach can also improve performance and recovery time. For more information, see [MySQL file size limits in Amazon RDS \(p. 1437\)](#).

Very large tables (greater than 100 GB in size) can negatively affect performance for both reads and writes (including DML statements and especially DDL statements). Indexes on large tables can significantly improve select performance, but they can also degrade the performance of DML statements. DDL statements, such as ALTER TABLE, can be significantly slower for the large tables because those operations might completely rebuild a table in some cases. These DDL statements might lock the tables for the duration of the operation.

The amount of memory required by MySQL for reads and writes depends on the tables involved in the operations. It is a best practice to have at least enough RAM to hold the indexes of *actively used* tables. To find the ten largest tables and indexes in a database, use the following query:

```
select table_schema, TABLE_NAME, dat, idx from
(SELECT table_schema, TABLE_NAME,
      ( data_length ) / 1024 / 1024 as dat,
      ( index_length ) / 1024 / 1024 as idx
FROM information_schema.TABLES
order by 3 desc ) a
order by 3 desc
limit 10;
```

Number of tables

Your underlying file system might have a limit on the number of files that represent tables. However, MySQL has no limit on the number of tables. Despite this, the total number of tables in the MySQL InnoDB storage engine can contribute to the performance degradation, regardless of the size of those tables. To limit the operating system impact, you can split the tables across multiple databases in the same MySQL DB instance. Doing so might limit the number of files in a directory but won't solve the overall problem.

When there is performance degradation because of a large number of tables (more than 10 thousand), it is caused by MySQL working with storage files, including opening and closing them. To address this issue, you can increase the size of the table_open_cache and table_definition_cache parameters. However, increasing the values of those parameters might significantly increase the amount of memory MySQL uses, and might even use all of the available memory. For more information, see [How MySQL Opens and Closes Tables](#) in the MySQL documentation.

In addition, too many tables can significantly affect MySQL startup time. Both a clean shutdown and restart and a crash recovery can be affected, especially in versions prior to MySQL 8.0.

We recommend having fewer than 10,000 tables total across all of the databases in a DB instance. For a use case with a large number of tables in a MySQL database, see [One Million Tables in MySQL 8.0](#).

Storage engine

The point-in-time restore and snapshot restore features of Amazon RDS for MySQL require a crash-recoverable storage engine. These features are supported for the InnoDB storage engine only. Although MySQL supports multiple storage engines with varying capabilities, not all of them are optimized for crash recovery and data durability. For example, the MyISAM storage engine doesn't support reliable crash recovery and might prevent a point-in-time restore or snapshot restore from working as intended. This might result in lost or corrupt data when MySQL is restarted after a crash.

InnoDB is the recommended and supported storage engine for MySQL DB instances on Amazon RDS. InnoDB instances can also be migrated to Aurora, while MyISAM instances can't be migrated. However, MyISAM performs better than InnoDB if you require intense, full-text search capability. If you still choose to use MyISAM with Amazon RDS, following the steps outlined in [Automated backups with unsupported MySQL storage engines \(p. 435\)](#) can be helpful in certain scenarios for snapshot restore functionality.

If you want to convert existing MyISAM tables to InnoDB tables, you can use the process outlined in the [MySQL documentation](#). MyISAM and InnoDB have different strengths and weaknesses, so you should fully evaluate the impact of making this switch on your applications before doing so.

In addition, Federated Storage Engine is currently not supported by Amazon RDS for MySQL.

Best practices for working with MariaDB

Both table sizes and number of tables in a MariaDB database can affect performance.

Table size

Typically, operating system constraints on file sizes determine the effective maximum table size for MariaDB databases. So, the limits usually aren't determined by internal MariaDB constraints.

On a MariaDB DB instance, avoid tables in your database growing too large. Although the general storage limit is 64 TiB, provisioned storage limits restrict the maximum size of a MariaDB table file to 16 TiB. Partition your large tables so that file sizes are well under the 16 TiB limit. This approach can also improve performance and recovery time.

Very large tables (greater than 100 GB in size) can negatively affect performance for both reads and writes (including DML statements and especially DDL statements). Indexes on large tables can significantly improve select performance, but they can also degrade the performance of DML statements. DDL statements, such as ALTER TABLE, can be significantly slower for the large tables because those operations might completely rebuild a table in some cases. These DDL statements might lock the tables for the duration of the operation.

The amount of memory required by MariaDB for reads and writes depends on the tables involved in the operations. It is a best practice to have at least enough RAM to hold the indexes of *actively* used tables. To find the ten largest tables and indexes in a database, use the following query:

```
select table_schema, TABLE_NAME, dat, idx from
(SELECT table_schema, TABLE_NAME,
      ( data_length ) / 1024 / 1024 as dat,
      ( index_length ) / 1024 / 1024 as idx
FROM information_schema.TABLES
order by 3 desc ) a
order by 3 desc
limit 10;
```

Number of tables

Your underlying file system might have a limit on the number of files that represent tables. However, MariaDB has no limit on the number of tables. Despite this, the total number of tables in the MariaDB InnoDB storage engine can contribute to the performance degradation, regardless of the size of those tables. To limit the operating system impact, you can split the tables across multiple databases in the same MariaDB DB instance. Doing so might limit the number of files in a directory but doesn't solve the overall problem.

When there is performance degradation because of a large number of tables (more than 10,000), it's caused by MariaDB working with storage files. This work includes MariaDB opening and closing storage files. To address this issue, you can increase the size of the `table_open_cache` and `table_definition_cache` parameters. However, increasing the values of those parameters might significantly increase the amount of memory MariaDB uses. It might even use all of the available memory. For more information, see [Optimizing table_open_cache](#) in the MariaDB documentation.

In addition, too many tables can significantly affect MariaDB startup time. Both a clean shutdown and restart and a crash recovery can be affected. We recommend having fewer than ten thousand tables total across all of the databases in a DB instance.

Storage engine

The point-in-time restore and snapshot restore features of Amazon RDS for MariaDB require a crash-recoverable storage engine. Although MariaDB supports multiple storage engines with varying capabilities, not all of them are optimized for crash recovery and data durability. For example, although Aria is a crash-safe replacement for MyISAM, it might still prevent a point-in-time restore or snapshot restore from working as intended. This might result in lost or corrupt data when MariaDB is restarted after a crash. InnoDB is the recommended and supported storage engine for MariaDB DB instances on Amazon RDS. If you still choose to use Aria with Amazon RDS, following the steps outlined in [Automated backups with unsupported MariaDB storage engines \(p. 436\)](#) can be helpful in certain scenarios for snapshot restore functionality.

If you want to convert existing MyISAM tables to InnoDB tables, you can use the process outlined in the [MariaDB documentation](#). MyISAM and InnoDB have different strengths and weaknesses, so you should fully evaluate the impact of making this switch on your applications before doing so.

Best practices for working with Oracle

For information about best practices for working with Amazon RDS for Oracle, see [Best practices for running Oracle database on Amazon Web Services](#).

A 2020 AWS virtual workshop included a presentation on running production Oracle databases on Amazon RDS. A video of the presentation is available [here](#).

Best practices for working with PostgreSQL

Of two important areas where you can improve performance with RDS for PostgreSQL, one is when loading data into a DB instance. Another is when using the PostgreSQL autovacuum feature. The following sections cover some of the practices we recommend for these areas.

For information on how Amazon RDS implements other common PostgreSQL DBA tasks, see [Common DBA tasks for Amazon RDS for PostgreSQL \(p. 1915\)](#).

Loading data into a PostgreSQL DB instance

When loading data into an Amazon RDS for PostgreSQL DB instance, modify your DB instance settings and your DB parameter group values. Set these to allow for the most efficient importing of data into your DB instance.

Modify your DB instance settings to the following:

- Disable DB instance backups (set `backup_retention` to 0)
- Disable Multi-AZ

Modify your DB parameter group to include the following settings. Also, test the parameter settings to find the most efficient settings for your DB instance.

- Increase the value of the `maintenance_work_mem` parameter. For more information about PostgreSQL resource consumption parameters, see the [PostgreSQL documentation](#).
- Increase the value of the `max_wal_size` and `checkpoint_timeout` parameters to reduce the number of writes to the write-ahead log (WAL) log.
- Disable the `synchronous_commit` parameter.
- Disable the PostgreSQL autovacuum parameter.
- Make sure that none of the tables you're importing are unlogged. Data stored in unlogged tables can be lost during a failover. For more information, see [CREATE TABLE UNLOGGED](#).

Use the `pg_dump -Fc` (compressed) or `pg_restore -j` (parallel) commands with these settings.

After the load operation completes, return your DB instance and DB parameters to their normal settings.

Working with the PostgreSQL autovacuum feature

The autovacuum feature for PostgreSQL databases is a feature that we strongly recommend you use to maintain the health of your PostgreSQL DB instance. Autovacuum automates the execution of the `VACUUM` and `ANALYZE` command. Using autovacuum is required by PostgreSQL, not imposed by Amazon RDS, and its use is critical to good performance. The feature is enabled by default for all new Amazon RDS for PostgreSQL DB instances, and the related configuration parameters are appropriately set by default.

Your database administrator needs to know and understand this maintenance operation. For the PostgreSQL documentation on autovacuum, see [The Autovacuum Daemon](#).

Autovacuum is not a "resource free" operation, but it works in the background and yields to user operations as much as possible. When enabled, autovacuum checks for tables that have had a large number of updated or deleted tuples. It also protects against loss of very old data due to transaction ID wraparound. For more information, see [Preventing transaction ID wraparound failures](#).

Autovacuum should not be thought of as a high-overhead operation that can be reduced to gain better performance. On the contrary, tables that have a high velocity of updates and deletes will quickly deteriorate over time if autovacuum is not run.

Important

Not running autovacuum can result in an eventual required outage to perform a much more intrusive vacuum operation. In some cases, an RDS for PostgreSQL DB instance might become unavailable because of an over-conservative use of autovacuum. In these cases, the PostgreSQL database shuts down to protect itself. At that point, Amazon RDS must perform a single-user-mode full vacuum directly on the DB instance. This full vacuum can result in a multi-hour

outage. Thus, we strongly recommend that you do not turn off autovacuum, which is turned on by default.

The autovacuum parameters determine when and how hard autovacuum works. The `autovacuum_vacuum_threshold` and `autovacuum_vacuum_scale_factor` parameters determine when autovacuum is run. The `autovacuum_max_workers`, `autovacuum_nap_time`, `autovacuum_cost_limit`, and `autovacuum_cost_delay` parameters determine how hard autovacuum works. For more information about autovacuum, when it runs, and what parameters are required, see [Routine Vacuuming](#) in the PostgreSQL documentation.

The following query shows the number of "dead" tuples in a table named `table1`:

```
PROMPT> select relname, n_dead_tup, last_vacuum, last_autovacuum from pg_catalog.pg_stat_all_tables where n_dead_tup > 0 and relname = 'table1';
```

The results of the query will resemble the following:

relname	n_dead_tup	last_vacuum	last_autovacuum
tasks	81430522		

(1 row)

Amazon RDS for PostgreSQL best practices video

The 2020 AWS re:Invent conference included a presentation on new features and best practices for working with PostgreSQL on Amazon RDS. A video of the presentation is available [here](#).

Best practices for working with SQL Server

Best practices for a Multi-AZ deployment with a SQL Server DB instance include the following:

- Use Amazon RDS DB events to monitor failovers. For example, you can be notified by text message or email when a DB instance fails over. For more information about Amazon RDS events, see [Working with Amazon RDS event notification \(p. 650\)](#).
- If your application caches DNS values, set time to live (TTL) to less than 30 seconds. Setting TTL as so is a good practice in case there is a failover. In a failover, the IP address might change and the cached value might no longer be in service.
- We recommend that you *do not* enable the following modes because they turn off transaction logging, which is required for Multi-AZ:
 - Simple recover mode
 - Offline mode
 - Read-only mode
- Test to determine how long it takes for your DB instance to failover. Failover time can vary due to the type of database, the instance class, and the storage type you use. You should also test your application's ability to continue working if a failover occurs.
- To shorten failover time, do the following:
 - Ensure that you have sufficient Provisioned IOPS allocated for your workload. Inadequate I/O can lengthen failover times. Database recovery requires I/O.
 - Use smaller transactions. Database recovery relies on transactions, so if you can break up large transactions into multiple smaller transactions, your failover time should be shorter.

- Take into consideration that during a failover, there will be elevated latencies. As part of the failover process, Amazon RDS automatically replicates your data to a new standby instance. This replication means that new data is being committed to two different DB instances. So there might be some latency until the standby DB instance has caught up to the new primary DB instance.
- Deploy your applications in all Availability Zones. If an Availability Zone does go down, your applications in the other Availability Zones will still be available.

When working with a Multi-AZ deployment of SQL Server, remember that Amazon RDS creates replicas for all SQL Server databases on your instance. If you don't want specific databases to have secondary replicas, set up a separate DB instance that doesn't use Multi-AZ for those databases.

Amazon RDS for SQL Server best practices video

The 2019 AWS re:Invent conference included a presentation on new features and best practices for working with SQL Server on Amazon RDS. A video of the presentation is available [here](#).

Working with DB parameter groups

We recommend that you try out DB parameter group changes on a test DB instance before applying parameter group changes to your production DB instances. Improperly setting DB engine parameters in a DB parameter group can have unintended adverse effects, including degraded performance and system instability. Always exercise caution when modifying DB engine parameters and back up your DB instance before modifying a DB parameter group.

For information about backing up your DB instance, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

Best practices for automating DB instance creation

It's an Amazon RDS best practice to create a DB instance with the preferred minor version of the database engine. You can use the AWS CLI, Amazon RDS API, or AWS CloudFormation to automate DB instance creation. When you use these methods, you can specify only the major version and Amazon RDS automatically creates the instance with the preferred minor version. For example, if PostgreSQL 12.5 is the preferred minor version, and if you specify version 12 with `create-db-instance`, the DB instance will be version 12.5.

To determine the preferred minor version, you can run the `describe-db-engine-versions` command with the `--default-only` option as shown in the following example.

```
aws rds describe-db-engine-versions --default-only --engine postgres
{
    "DBEngineVersions": [
        {
            "Engine": "postgres",
            "EngineVersion": "12.5",
            "DBParameterGroupFamily": "postgres12",
            "DBEngineDescription": "PostgreSQL",
            "DBEngineVersionDescription": "PostgreSQL 12.5-R1",
            "...some output truncated..."
        }
    ]
}
```

For information on creating DB instances programmatically, see the following resources:

- Using the AWS CLI – [create-db-instance](#)
- Using the Amazon RDS API – [CreateDBInstance](#)
- Using AWS CloudFormation – [AWS::RDS::DBInstance](#)

Amazon RDS new features and best practices presentation video

The 2019 AWS re:Invent conference included a presentation on new Amazon RDS features and best practices for monitoring, analyzing, and tuning database performance using RDS. A video of the presentation is available [here](#).

Configuring an Amazon RDS DB instance

This section shows how to set up your Amazon RDS DB instance. Before creating a DB instance, decide on the DB instance class that will run the DB instance. Also, decide where the DB instance will run by choosing an AWS Region. Next, create the DB instance.

You can configure a DB instance with an option group and a DB parameter group.

- An *option group* specifies features, called options, that are available for a particular Amazon RDS DB instance.
- A *DB parameter group* acts as a container for engine configuration values that are applied to one or more DB instances.

The options and parameters that are available depend on the DB engine and DB engine version. You can specify an option group and a DB parameter group when you create a DB instance. You can also modify a DB instance to specify them.

Topics

- [Creating an Amazon RDS DB instance \(p. 230\)](#)
- [Creating a Multi-AZ DB cluster \(p. 252\)](#)
- [Creating Amazon RDS resources with AWS CloudFormation \(p. 266\)](#)
- [Connecting to an Amazon RDS DB instance \(p. 267\)](#)
- [Working with option groups \(p. 273\)](#)
- [Working with parameter groups \(p. 289\)](#)

Creating an Amazon RDS DB instance

The basic building block of Amazon RDS is the DB instance, where you create your databases. You choose the engine-specific characteristics of the DB instance when you create it. You also choose the storage capacity, CPU, memory, and so on, of the AWS instance on which the database server runs.

Topics

- [DB instance prerequisites \(p. 230\)](#)
- [Creating a DB instance \(p. 233\)](#)
- [Settings for DB instances \(p. 237\)](#)

DB instance prerequisites

Important

Before you can create an Amazon RDS DB instance, you must complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

The following are prerequisites to complete before creating a DB instance.

Topics

- [Configure the network for the DB instance \(p. 230\)](#)
- [Additional prerequisites \(p. 233\)](#)

Configure the network for the DB instance

You can create an Amazon RDS DB instance only in a virtual private cloud (VPC) based on the Amazon VPC service. Also, it must be in an AWS Region that has at least two Availability Zones. The DB subnet group that you choose for the DB instance must cover at least two Availability Zones. This configuration ensures that you can configure a Multi-AZ deployment when you create the DB instance or easily move to one in the future.

To set up connectivity between your new DB instance and an Amazon EC2 instance in the same VPC, do so when you create the DB instance. To connect to your DB instance from resources other than EC2 instances in the same VPC, configure the network connections manually.

Topics

- [Configure automatic network connectivity with an EC2 instance \(p. 230\)](#)
- [Configure the network manually \(p. 232\)](#)

Configure automatic network connectivity with an EC2 instance

When you create an RDS DB instance, you can use the AWS Management Console to set up connectivity between an EC2 instance and the new DB instance. When you do so, RDS configures your VPC and network settings automatically. The DB instance is created in the same VPC as the EC2 instance so that the EC2 instance can access the DB instance.

The following are requirements for connecting an EC2 instance with the DB instance:

- The EC2 instance must exist in the AWS Region before you create the DB instance.

If no EC2 instances exist in the AWS Region, the console provides a link to create one.

- The user who is creating the DB instance must have permissions to perform the following operations:
 - ec2:AssociateRouteTable
 - ec2:AuthorizeSecurityGroupEgress
 - ec2>CreateRouteTable
 - ec2>CreateSubnet
 - ec2>CreateSecurityGroup
 - ec2:DescribeInstances
 - ec2:DescribeNetworkInterfaces
 - ec2:DescribeRouteTables
 - ec2:DescribeSecurityGroups
 - ec2:DescribeSubnets
 - ec2:ModifyNetworkInterfaceAttribute
 - ec2:RevokeSecurityGroupEgress

Using this option creates a private DB instance. The DB instance uses a DB subnet group with only private subnets to restrict access to resources within the VPC.

To connect an EC2 instance to the DB instance, choose **Connect to an EC2 compute resource** in the **Connectivity** section on the [Create database](#) page.

Connectivity Info C

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

EC2 Instance Info
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

[Choose EC2 instances](#) ▼

When you choose **Connect to an EC2 compute resource**, RDS sets the following options automatically. You can't change these settings unless you choose not to set up connectivity with an EC2 instance by choosing **Don't connect to an EC2 compute resource**.

Console option	Automatic setting
Network type	RDS sets network type to IPv4 . Currently, dual-stack mode isn't supported when you set up a connection between an EC2 instance and the DB instance.
Virtual Private Cloud (VPC)	RDS sets the VPC to the one associated with the EC2 instance.
DB subnet group	A DB subnet group with a private subnet in each Availability Zone in the AWS Region is required. If a DB subnet group that meets this requirement exists, RDS uses the existing DB subnet group.

Console option	Automatic setting
	<p>In some cases, a DB subnet group that meets this requirement doesn't exist. If not, RDS uses an available private subnet in each Availability Zone to create a DB subnet group using the private subnets. If a private subnet isn't available in an Availability Zone, RDS creates a private subnet in the Availability Zone. RDS then creates the DB subnet group.</p> <p>When a private subnet is available, RDS uses the route table associated with it. RDS then adds any subnets it creates to this route table. When no private subnet is available, RDS creates a route table with no internet gateway access. RDS then adds the subnets it creates to the route table.</p>
Public access	<p>RDS chooses No so that the DB instance isn't publicly accessible.</p> <p>For security, it is a best practice to keep the database private and make sure it isn't accessible from the internet.</p>
VPC security group (firewall)	<p>RDS creates a new security group that is associated with the DB instance. The security group is named <code>rds-ec2-n</code>, where <code>n</code> is a number. This security group includes an inbound rule with the EC2 VPC security group (firewall) as the source. This security group that is associated with the DB instance allows the EC2 instance to access the DB instance.</p> <p>RDS also creates a new security group that is associated with the EC2 instance. The security group is named <code>ec2-rds-n</code>, where <code>n</code> is a number. This security group includes an outbound rule with the VPC security group of the DB instance as the source. This security group allows the EC2 instance to send traffic to the DB instance.</p> <p>You can add another new security group by choosing Create new and typing the name of the new security group.</p> <p>You can add existing security groups by choosing Choose existing and selecting security groups to add.</p>
Availability Zone	<p>When you choose Single DB instance in Availability & durability (Single-AZ deployment), RDS chooses the Availability Zone of the EC2 instance.</p> <p>When you choose Multi-AZ DB instance in Availability & durability (Multi-AZ DB instance deployment), RDS chooses the Availability Zone of the EC2 instance for one DB instance in the deployment. RDS randomly chooses a different Availability Zone for the other DB instance. Either the primary DB instance or the standby replica is created in the same Availability Zone as the EC2 instance. When you choose Multi-AZ DB instance, there is the possibility of cross Availability Zone costs if the DB instance and EC2 instance are in different Availability Zones.</p>

For more information about these settings, see [Settings for DB instances \(p. 237\)](#).

If you change these settings after the DB instance is created, the changes might affect the connection between the EC2 instance and the DB instance.

Configure the network manually

To connect to your DB instance from resources other than EC2 instances in the same VPC, configure the network connections manually. If you use the AWS Management Console to create your DB instance, you can have Amazon RDS automatically create a VPC for you. Or you can use an existing VPC or create a

new VPC for your DB instance. With any approach, your VPC requires at least one subnet in each of at least two Availability Zones for use with an RDS DB instance.

By default, Amazon RDS creates the DB instance in an Availability Zone automatically for you. To choose a specific Availability Zone, you need to change the **Availability & durability** setting to **Single DB instance**. Doing so exposes an **Availability Zone** setting that lets you choose from among the Availability Zones in your VPC. However, if you choose a Multi-AZ deployment, RDS chooses the Availability Zone of the primary or writer DB instance automatically, and the **Availability Zone** setting doesn't appear.

In some cases, you might not have a default VPC or haven't created a VPC. In these cases, you can have Amazon RDS automatically create a VPC for you when you create a DB instance using the console. Otherwise, do the following:

- Create a VPC with at least one subnet in each of at least two of the Availability Zones in the AWS Region where you want to deploy your DB instance. For more information, see [Working with a DB instance in a VPC \(p. 2104\)](#) and [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).
- Specify a VPC security group that authorizes connections to your DB instance. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#) and [Controlling access with security groups \(p. 2085\)](#).
- Specify an RDS DB subnet group that defines at least two subnets in the VPC that can be used by the DB instance. For more information, see [Working with DB subnet groups \(p. 2104\)](#).

Additional prerequisites

Before you create your DB instance, consider the following additional prerequisites:

- If you are connecting to AWS using AWS Identity and Access Management (IAM) credentials, your AWS account must have certain IAM policies. These grant the permissions required to perform Amazon RDS operations. For more information, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

To use IAM to access the RDS console, sign in to the AWS Management Console with your IAM user credentials. Then go to the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

- To tailor the configuration parameters for your DB instance, specify a DB parameter group with the required parameter settings. For information about creating or modifying a DB parameter group, see [Working with parameter groups \(p. 289\)](#).
- Determine the TCP/IP port number to specify for your DB instance. The firewalls at some companies block connections to the default ports for RDS DB instances. If your company firewall blocks the default port, choose another port for your DB instance.

Creating a DB instance

You can create an Amazon RDS DB instance using the AWS Management Console, the AWS CLI, or the RDS API.

Console

You can create a DB instance by using the AWS Management Console with **Easy create** enabled or not enabled. With **Easy create** enabled, you specify only the DB engine type, DB instance size, and DB instance identifier. **Easy create** uses the default setting for other configuration options. With **Easy create** not enabled, you specify more configuration options when you create a database, including ones for availability, security, backups, and maintenance.

Note

In the following procedure, **Standard create** is enabled, and **Easy create** isn't enabled. This procedure uses Microsoft SQL Server as an example.

For examples that use **Easy create** to walk you through creating and connecting to sample DB instances for each engine, see [Getting started with Amazon RDS \(p. 153\)](#).

To create a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.
5. In **Choose a database creation method**, select **Standard Create**.
6. In **Engine options**, choose the engine type: MariaDB, Microsoft SQL Server, MySQL, Oracle, or PostgreSQL. **Microsoft SQL Server** is shown here.

Create database

Choose a database creation method Info

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type Info

Amazon Aurora 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

Edition

SQL Server Express Edition
Affordable database management system that supports database sizes up to 10 GB.

SQL Server Web Edition
In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.

SQL Server Standard Edition
Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.

SQL Server Enterprise Edition
For more information about the editions, see [Editions and features](#).

7. For **Edition**, if you're using Oracle or SQL Server choose the DB engine edition that you want to use.

MySQL has only one option for the edition, and MariaDB and PostgreSQL have none.

8. For **Version**, choose the engine version.
9. In **Templates**, choose the template that matches your use case. If you choose **Production**, the following are preselected in a later step:
 - **Multi-AZ failover option**
 - **Provisioned IOPS SSD (io1) storage option**
 - **Enable deletion protection** option

We recommend these features for any production environment.

Note

Template choices vary by edition.

10. To enter your master password, do the following:
 - a. In the **Settings** section, open **Credential Settings**.
 - b. If you want to specify a password, clear the **Auto generate a password** check box if it is selected.
 - c. (Optional) Change the **Master username** value.
 - d. Enter the same password in **Master password** and **Confirm password**.
11. (Optional) Set up a connection to a compute resource for this DB instance.

You can configure connectivity between an Amazon EC2 instance and the new DB instance during DB instance creation. For more information, see [Configure automatic network connectivity with an EC2 instance \(p. 230\)](#).

12. For the remaining sections, specify your DB instance settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).
13. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB instance, choose **View credential details**.

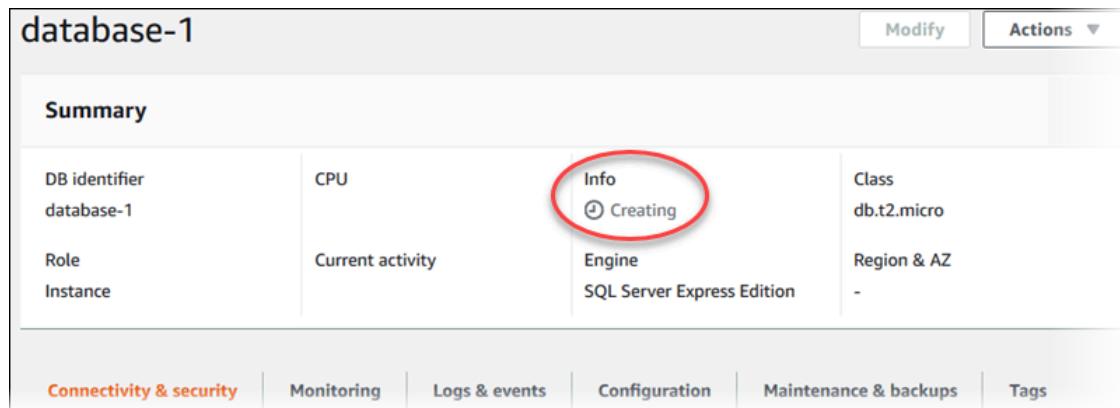
To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it. If you need to change the master user password after the DB instance is available, modify the DB instance to do so. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

14. For **Databases**, choose the name of the new DB instance.

On the RDS console, the details for the new DB instance appear. The DB instance has a status of **Creating** until the DB instance is created and ready for use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and storage allocated, it can take several minutes for the new instance to be available.



AWS CLI

To create a DB instance by using the AWS CLI, call the [create-db-instance](#) command with the following parameters:

- `--db-instance-identifier`
- `--db-instance-class`
- `--vpc-security-group-ids`
- `--db-subnet-group`
- `--engine`
- `--master-username`
- `--master-user-password`
- `--allocated-storage`
- `--backup-retention-period`

For information about each setting, see [Settings for DB instances \(p. 237\)](#).

This example uses Microsoft SQL Server.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--engine sqlserver-se \
--db-instance-identifier mymssqlserver \
--allocated-storage 250 \
--db-instance-class db.t3.large \
--vpc-security-group-ids mysecuritygroup \
--db-subnet-group mydbsubnetgroup \
--master-username masterawsuser \
--master-user-password masteruserpassword \
--backup-retention-period 3
```

For Windows:

```
aws rds create-db-instance ^
--engine sqlserver-se ^
--db-instance-identifier mydbinstance ^
--allocated-storage 250 ^
```

```
--db-instance-class db.t3.large ^
--vpc-security-group-ids mysecuritygroup ^
--db-subnet-group mydbsubnetgroup ^
--master-username masterawsuser ^
--master-user-password masteruserpassword ^
--backup-retention-period 3
```

This command produces output similar to the following.

```
DBINSTANCE mydbinstance db.t3.large sqlserver-se 250 sa creating 3 **** n
10.50.2789
SECGROUP default active
PARAMGRP default.sqlserver-se-14 in-sync
```

RDS API

To create a DB instance by using the Amazon RDS API, call the [CreateDBInstance](#) operation.

For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Settings for DB instances

In the following table, you can find details about settings that you choose when you create a DB instance. The table also shows the DB engines for which each setting is supported.

You can create a DB instance using the console, the [create-db-instance](#) CLI command, or the [CreateDBInstance](#) RDS API operation.

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Allocated storage	<p>The amount of storage to allocate for your DB instance (in gibibytes). In some cases, allocating a higher amount of storage for your DB instance than the size of your database can improve I/O performance.</p> <p>For more information, see Amazon RDS DB instance storage (p. 64).</p>	CLI option: --allocated-storage API parameter: AllocatedStorage	All
Architecture settings	<p>The architecture of the database: CDB (single-tenant) or non-CDB. Oracle Database 21c uses CDB architecture only. Oracle Database 19c can use either CDB or non-CDB architecture. Releases lower than Oracle Database 19c use non-CDB only.</p> <p>If you choose Use multitenant architecture, RDS for Oracle creates a container database (CDB). This CDB contains one pluggable database (PDB). If you don't choose this option, RDS for Oracle creates</p>	CLI option: --engine oracle-ee-cdb (multitenant) --engine oracle-se2-cdb (multitenant) --engine oracle-ee (traditional) --engine oracle-se2 (traditional) API parameter: Engine	Oracle

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
	<p>a non-CDB. A non-CDB uses the traditional Oracle architecture.</p> <p>For more information, see RDS for Oracle architecture (p. 1480).</p>		
Auto minor version upgrade	<p>Enable auto minor version upgrade to enable your DB instance to receive preferred minor DB engine version upgrades automatically when they become available. Amazon RDS performs automatic minor version upgrades in the maintenance window.</p> <p>For more information, see Automatically upgrading the minor engine version (p. 362).</p>	CLI option: --auto-minor-version-upgrade --no-auto-minor-version-upgrade API parameter: AutoMinorVersionUpgrade	All
Availability zone	<p>The Availability Zone for your DB instance. Use the default value of No Preference unless you want to specify an Availability Zone.</p> <p>For more information, see Regions, Availability Zones, and Local Zones (p. 72).</p>	CLI option: --availability-zone API parameter: AvailabilityZone	All
AWS KMS key	Only available if Encryption is set to Enable encryption . Choose the AWS KMS key to use for encrypting this DB instance. For more information, see Encrypting Amazon RDS resources (p. 2000) .	CLI option: --kms-key-id API parameter: KmsKeyId	All
Backup replication	<p>Choose Enable replication in another AWS Region to create backups in an additional Region for disaster recovery.</p> <p>Then choose the Destination Region for the additional backups.</p>	Not available when creating a DB instance. For information on enabling cross-Region backups using the AWS CLI or RDS API, see Enabling cross-Region automated backups (p. 439) .	Oracle PostgreSQL SQL Server
Backup retention period	<p>The number of days that you want automatic backups of your DB instance to be retained. For any nontrivial DB instance, set this value to 1 or greater.</p> <p>For more information, see Working with backups (p. 427).</p>	CLI option: --backup-retention-period API parameter: BackupRetentionPeriod	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Backup target	<p>Choose AWS Cloud to store automated backups and manual snapshots in the parent AWS Region. Choose Outposts (on-premises) to store them locally on your Outpost.</p> <p>This option setting applies only to RDS on Outposts. For more information, see Creating DB instances for Amazon RDS on AWS Outposts (p. 914).</p>	CLI option: <code>--backup-target</code> API parameter: <code>BackupTarget</code>	MySQL, PostgreSQL, SQL Server
Backup window	<p>The time period during which Amazon RDS automatically takes a backup of your DB instance. Unless you have a specific time that you want to have your database backed up, use the default of No Preference.</p> <p>For more information, see Working with backups (p. 427).</p>	CLI option: <code>--preferred-backup-window</code> API parameter: <code>PreferredBackupWindow</code>	All
Character set	<p>The character set for your DB instance. The default value of AL32UTF8 for the DB character set is for the Unicode 5.0 UTF-8 Universal character set. You can't change the DB character set after you create the DB instance.</p> <p>In a single-tenant configuration, a non-default DB character set affects only the PDB, not the CDB. For more information, see RDS for Oracle architecture (p. 1480).</p> <p>The DB character set is different from the national character set, which is called the NCHAR character set. Unlike the DB character set, the NCHAR character set specifies the encoding for NCHAR data types (NCHAR, NVARCHAR2, and NCLOB) columns without affecting database metadata.</p> <p>For more information, see RDS for Oracle character sets (p. 1482).</p>	CLI option: <code>--character-set-name</code> API parameter: <code>CharacterSetName</code>	Oracle

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Collation	A server-level collation for your DB instance. For more information, see Server-level collation for Microsoft SQL Server (p. 1296) .	CLI option: --character-set-name API parameter: CharacterSetName	SQL Server
Copy tags to snapshots	This option copies any DB instance tags to a DB snapshot when you create a snapshot. For more information, see Tagging Amazon RDS resources (p. 392) .	CLI option: --copy-tags-to-snapshot --no-copy-tags-to-snapshot RDS API parameter: CopyTagsToSnapshot	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Database authentication	<p>The database authentication option that you want to use.</p> <p>Choose Password authentication to authenticate database users with database passwords only.</p> <p>Choose Password and IAM DB authentication to authenticate database users with database passwords and user credentials through IAM users and roles. For more information, see IAM database authentication for MariaDB, MySQL, and PostgreSQL (p. 2048). This option is only supported for MySQL and PostgreSQL.</p> <p>Choose Password and Kerberos authentication to authenticate database users with database passwords and Kerberos authentication through an AWS Managed Microsoft AD created with AWS Directory Service. Next, choose the directory or choose Create a new Directory.</p> <p>For more information, see one of the following:</p> <ul style="list-style-type: none"> • Using Kerberos authentication for MySQL (p. 1333) • Configuring Kerberos authentication for Amazon RDS for Oracle (p. 1501) • Using Kerberos authentication with Amazon RDS for PostgreSQL (p. 1823) 	<p>IAM:</p> <p>CLI option:</p> <pre>--enable-iam-database-authentication</pre> <p>RDS API parameter:</p> <pre>EnableIAMDatabaseAuthentication</pre> <p>Kerberos:</p> <p>CLI option:</p> <pre>--domain</pre> <pre>--domain-iam-role-name</pre> <p>RDS API parameter:</p> <pre>Domain</pre> <pre>DomainIAMRoleName</pre>	Varies by authentication type
Database management type	<p>Choose Amazon RDS if you don't need to customize your environment.</p> <p>Choose Amazon RDS Custom if you want to customize the database, OS, and infrastructure. For more information, see Working with Amazon RDS Custom (p. 755).</p>	For the CLI and API, you specify the database engine type.	Oracle SQL Server

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Database port	<p>The port that you want to access the DB instance through. The default port is shown.</p> <p>Note The firewalls at some companies block connections to the default MariaDB, MySQL, and PostgreSQL ports. If your company firewall blocks the default port, enter another port for your DB instance.</p>	<p>CLI option: --port</p> <p>RDS API parameter: Port</p>	All
DB engine version	The version of database engine that you want to use.	<p>CLI option: --engine-version</p> <p>RDS API parameter: EngineVersion</p>	All
DB instance class	<p>The configuration for your DB instance. For example, a db.t3.small DB instance class has 2 GiB memory, 2 vCPUs, 1 virtual core, a variable ECU, and a moderate I/O capacity.</p> <p>If possible, choose a DB instance class large enough that a typical query working set can be held in memory. When working sets are held in memory, the system can avoid writing to disk, which improves performance. For more information, see DB instance classes (p. 10).</p> <p>In RDS for Oracle, you can select Include additional memory configurations. These configurations are optimized for a high ratio of memory to vCPU. For example, db.r5.6xlarge.tpc2.mem4x is a db.r5.8x DB instance that has 2 threads per core (tpc2) and 4x the memory of a standard db.r5.6xlarge DB instance. For more information, see RDS for Oracle instance classes (p. 1477).</p>	<p>CLI option: --db-instance-class</p> <p>RDS API parameter: DBInstanceClass</p>	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
DB instance identifier	The name for your DB instance. Name your DB instances in the same way that you name your on-premises servers. Your DB instance identifier can contain up to 63 alphanumeric characters, and must be unique for your account in the AWS Region you chose.	CLI option: <code>--db-instance-identifier</code> RDS API parameter: <code>DBInstanceIdentifier</code>	All
DB parameter group	A parameter group for your DB instance. You can choose the default parameter group, or you can create a custom parameter group. For more information, see Working with parameter groups (p. 289) .	CLI option: <code>--db-parameter-group-name</code> RDS API parameter: <code>DBParameterGroupName</code>	All
DB subnet group	A DB subnet group to associate with this DB instance. For more information, see Working with DB subnet groups (p. 2104) .	CLI option: <code>--db-subnet-group-name</code> RDS API parameter: <code>DBSubnetGroupName</code>	All
Deletion protection	Enable deletion protection to prevent your DB instance from being deleted. If you create a production DB instance with the AWS Management Console, deletion protection is enabled by default. For more information, see Deleting a DB instance (p. 421) .	CLI option: <code>--deletion-protection</code> <code>--no-deletion-protection</code> RDS API parameter: <code>DeletionProtection</code>	All
Encryption	Enable Encryption to enable encryption at rest for this DB instance. For more information, see Encrypting Amazon RDS resources (p. 2000) .	CLI option: <code>--storage-encrypted</code> <code>--no-storage-encrypted</code> RDS API parameter: <code>StorageEncrypted</code>	All
Enhanced Monitoring	Enable enhanced monitoring to enable gathering metrics in real time for the operating system that your DB instance runs on. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) .	CLI options: <code>--monitoring-interval</code> <code>--monitoring-role-arn</code> RDS API parameters: <code>MonitoringInterval</code> <code>MonitoringRoleArn</code>	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Engine type	Choose the database engine to be used for this DB instance.	CLI option: --engine RDS API parameter: Engine	All
Initial database name	<p>The name for the database on your DB instance. If you don't provide a name, Amazon RDS doesn't create a database on the DB instance (except for Oracle and PostgreSQL). The name can't be a word reserved by the database engine, and has other constraints depending on the DB engine.</p> <p>MariaDB and MySQL:</p> <ul style="list-style-type: none"> It must contain 1–64 alphanumeric characters. <p>Oracle:</p> <ul style="list-style-type: none"> It must contain 1–8 alphanumeric characters. It can't be NULL. The default value is ORCL. It must begin with a letter. <p>PostgreSQL:</p> <ul style="list-style-type: none"> It must contain 1–63 alphanumeric characters. It must begin with a letter or an underscore. Subsequent characters can be letters, underscores, or digits (0–9). The initial database name is <code>postgres</code>. 	CLI option: --db-name RDS API parameter: DBName	All except SQL Server
License	<p>The license model:</p> <ul style="list-style-type: none"> Choose license-included for Microsoft SQL Server. Choose license-included or bring-your-own-license for Oracle. 	CLI option: --license-model RDS API parameter: LicenseModel	Oracle SQL Server

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Log exports	The types of database log files to publish to Amazon CloudWatch Logs. For more information, see Publishing database logs to Amazon CloudWatch Logs (p. 683) .	CLI option: --enable-cloudwatch-logs-exports RDS API parameter: EnableCloudwatchLogsExports	All
Maintenance window	The 30-minute window in which pending modifications to your DB instance are applied. If the time period doesn't matter, choose No Preference . For more information, see The Amazon RDS maintenance window (p. 354) .	CLI option: --preferred-maintenance-window RDS API parameter: PreferredMaintenanceWindow	All
Master password	The password for your master user account. The password has the following number of printable ASCII characters (excluding /, ", a space, and @) depending on the DB engine: <ul style="list-style-type: none">• Oracle: 8–30• MariaDB and MySQL: 8–41• SQL Server and PostgreSQL: 8–128	CLI option: --master-user-password RDS API parameter: MasterUserPassword	All
Master username	The name that you use as the master user name to log on to your DB instance with all database privileges. <ul style="list-style-type: none">• It can contain 1–16 alphanumeric characters and underscores.• Its first character must be a letter.• It can't be a word reserved by the database engine. You can't change the master user name after the DB instance is created. For more information on privileges granted to the master user, see Master user account privileges (p. 2087) .	CLI option: --master-username RDS API parameter: MasterUsername	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Microsoft SQL Server Windows Authentication	Enable Microsoft SQL Server Windows authentication , then Browse Directory to choose the directory where you want to allow authorized domain users to authenticate with this SQL Server instance using Windows Authentication.	CLI options: --domain --domain-iam-role-name RDS API parameters: Domain DomainIAMRoleName	SQL Server
Multi-AZ deployment	Create a standby instance to create a passive secondary replica of your DB instance in another Availability Zone for failover support. We recommend Multi-AZ for production workloads to maintain high availability. For development and testing, you can choose Do not create a standby instance . For more information, see Multi-AZ deployments for high availability (p. 121) .	CLI option: --multi-az --no-multi-az RDS API parameter: MultiAZ	All
National character set (NCHAR)	The national character set for your DB instance, commonly called the NCHAR character set. You can set the national character set to either AL16UTF16 (default) or UTF-8. You can't change the national character set after you create the DB instance. The national character set is different from the DB character set. Unlike the DB character set, the national character set specifies the encoding only for NCHAR data types (NCHAR, NVARCHAR2, and NCLOB) columns without affecting database metadata. For more information, see RDS for Oracle character sets (p. 1482) .	CLI option: --nchar-character-set-name API parameter: NcharCharacterSetName	Oracle

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Network type	<p>The IP addressing protocols supported by the DB instance.</p> <p>IPv4 (the default) to specify that resources can communicate with the DB instance only over the Internet Protocol version 4 (IPv4) addressing protocol.</p> <p>Dual-stack mode to specify that resources can communicate with the DB instance over IPv4, Internet Protocol version 6 (IPv6), or both. Use dual-stack mode if you have any resources that must communicate with your DB instance over the IPv6 addressing protocol. Also, make sure that you associate an IPv6 CIDR block with all subnets in the DB subnet group that you specify.</p> <p>For more information, see Amazon RDS IP addressing (p. 2105).</p>	<p>CLI option: <code>--network-type</code></p> <p>RDS API parameter: <code>NetworkType</code></p>	All
Option group	<p>An option group for your DB instance. You can choose the default option group or you can create a custom option group.</p> <p>For more information, see Working with option groups (p. 273).</p>	<p>CLI option: <code>--option-group-name</code></p> <p>RDS API parameter: <code>OptionGroupName</code></p>	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Performance Insights	<p>Enable Performance Insights to monitor your DB instance load so that you can analyze and troubleshoot your database performance.</p> <p>Choose a retention period to determine how much Performance Insights data history to keep. The retention setting in the free tier is Default (7 days). To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see Pricing and data retention for Performance Insights (p. 548).</p> <p>Choose a KMS key to use to protect the key used to encrypt this database volume. Choose from the KMS keys in your account, or enter the key from a different account.</p> <p>For more information, see Monitoring DB load with Performance Insights on Amazon RDS (p. 543).</p>	<p>CLI options:</p> <pre>--enable-performance-insights --no-enable-performance-insights --performance-insights-retention-period --performance-insights-kms-key-id</pre> <p>RDS API parameters:</p> <pre>EnablePerformanceInsights PerformanceInsightsRetentionPeriod PerformanceInsightsKMSKeyId</pre>	All
Provisioned IOPS	<p>The Provisioned IOPS (I/O operations per second) value for the DB instance. This setting is available only if you choose one of the following for Storage type:</p> <ul style="list-style-type: none"> • General purpose SSD (gp3) • Provisioned IOPS SSD (io1) <p>For more information, see Amazon RDS DB instance storage (p. 64).</p>	<p>CLI option:</p> <pre>--iops</pre> <p>RDS API parameter:</p> <pre>Iops</pre>	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Public access	<p>Yes to give the DB instance a public IP address, meaning that it's accessible outside the VPC. To be publicly accessible, the DB instance also has to be in a public subnet in the VPC.</p> <p>No to make the DB instance accessible only from inside the VPC.</p> <p>For more information, see Hiding a DB instance in a VPC from the internet (p. 2109).</p> <p>To connect to a DB instance from outside of its VPC, the DB instance must be publicly accessible. Also, access must be granted using the inbound rules of the DB instance's security group. In addition, other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 2141).</p> <p>If your DB instance isn't publicly accessible, use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 2015).</p>	<p>CLI option:</p> <pre>--publicly-accessible --no-publicly-accessible</pre> <p>RDS API parameter:</p> <pre>PubliclyAccessible</pre>	All
RDS Proxy	<p>Choose Create an RDS Proxy to create a proxy for your DB instance. Amazon RDS automatically creates an IAM role and a Secrets Manager secret for the proxy.</p> <p>For more information, see Using Amazon RDS Proxy (p. 921).</p>	Not available when creating a DB instance.	MariaDB MySQL PostgreSQL

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Storage autoscaling	<p>Enable storage autoscaling to enable Amazon RDS to automatically increase storage when needed to avoid having your DB instance run out of storage space.</p> <p>Use Maximum storage threshold to set the upper limit for Amazon RDS to automatically increase storage for your DB instance. The default is 1,000 GiB.</p> <p>For more information, see Managing capacity automatically with Amazon RDS storage autoscaling (p. 412).</p>	CLI option: <code>--max-allocated-storage</code> RDS API parameter: <code>MaxAllocatedStorage</code>	All
Storage throughput	<p>The storage throughput value for the DB instance. This setting is available only if you choose General purpose SSD (gp3) for Storage type.</p> <p>For more information, see Amazon RDS DB instance storage (p. 64).</p>	CLI option: <code>--storage-throughput</code> RDS API parameter: <code>StorageThroughput</code>	All
Storage type	<p>The storage type for your DB instance.</p> <p>If you choose General Purpose SSD (gp3), you can provision additional provisioned IOPS and storage throughput under Advanced settings.</p> <p>If you choose Provisioned IOPS SSD (io1), enter the Provisioned IOPS value.</p> <p>For more information, see Amazon RDS storage types (p. 64).</p>	CLI option: <code>--storage-type</code> RDS API parameter: <code>StorageType</code>	All
Subnet group	<p>A DB subnet group to associate with this DB instance.</p> <p>For more information, see Working with DB subnet groups (p. 2104).</p>	CLI option: <code>--db-subnet-group-name</code> RDS API parameter: <code>DBSubnetGroupName</code>	All

Console setting	Setting description	CLI option and RDS API parameter	Supported DB engines
Time zone	<p>The time zone for your DB instance. If you don't choose a time zone, your DB instance uses the default time zone. You can't change the time zone after the DB instance is created.</p> <p>For more information, see Local time zone for Microsoft SQL Server DB instances (p. 1074).</p>	<p>CLI option: <code>--timezone</code></p> <p>RDS API parameter: <code>Timezone</code></p>	SQL Server
Virtual Private Cloud (VPC)	<p>A VPC based on the Amazon VPC service to associate with this DB instance.</p> <p>For more information, see Amazon VPC VPCs and Amazon RDS (p. 2103).</p>	For the CLI and API, you specify the VPC security group IDs.	All
VPC security group (firewall)	<p>The security group to associate with the DB instance.</p> <p>For more information, see Overview of VPC security groups (p. 2085).</p>	<p>CLI option: <code>--vpc-security-group-ids</code></p> <p>RDS API parameter: <code>VpcSecurityGroupIds</code></p>	All

Creating a Multi-AZ DB cluster

A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones. Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower latency when compared to Multi-AZ deployments. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

Note

Multi-AZ DB clusters are supported only for the MySQL and PostgreSQL DB engines.

DB cluster prerequisites

Important

Before you can create a Multi-AZ DB cluster, you must complete the tasks in [Setting up for Amazon RDS \(p. 148\)](#).

The following are prerequisites to complete before creating a Multi-AZ DB cluster.

Topics

- [Configure the network for the DB cluster \(p. 252\)](#)
- [Additional prerequisites \(p. 255\)](#)

Configure the network for the DB cluster

You can create a Multi-AZ DB cluster only in a virtual private cloud (VPC) based on the Amazon VPC service. It must be in an AWS Region that has at least three Availability Zones. The DB subnet group that you choose for the DB cluster must cover at least three Availability Zones. This configuration ensures that each DB instance in the DB cluster is in a different Availability Zone.

To set up connectivity between your new DB cluster and an Amazon EC2 instance in the same VPC, do so when you create the DB cluster. To connect to your DB cluster from resources other than EC2 instances in the same VPC, configure the network connections manually.

Topics

- [Configure automatic network connectivity with an EC2 instance \(p. 252\)](#)
- [Configure the network manually \(p. 254\)](#)

Configure automatic network connectivity with an EC2 instance

When you create a Multi-AZ DB cluster, you can use the AWS Management Console to set up connectivity between an EC2 instance and the new DB cluster. When you do so, RDS configures your VPC and network settings automatically. The DB cluster is created in the same VPC as the EC2 instance so that the EC2 instance can access the DB cluster.

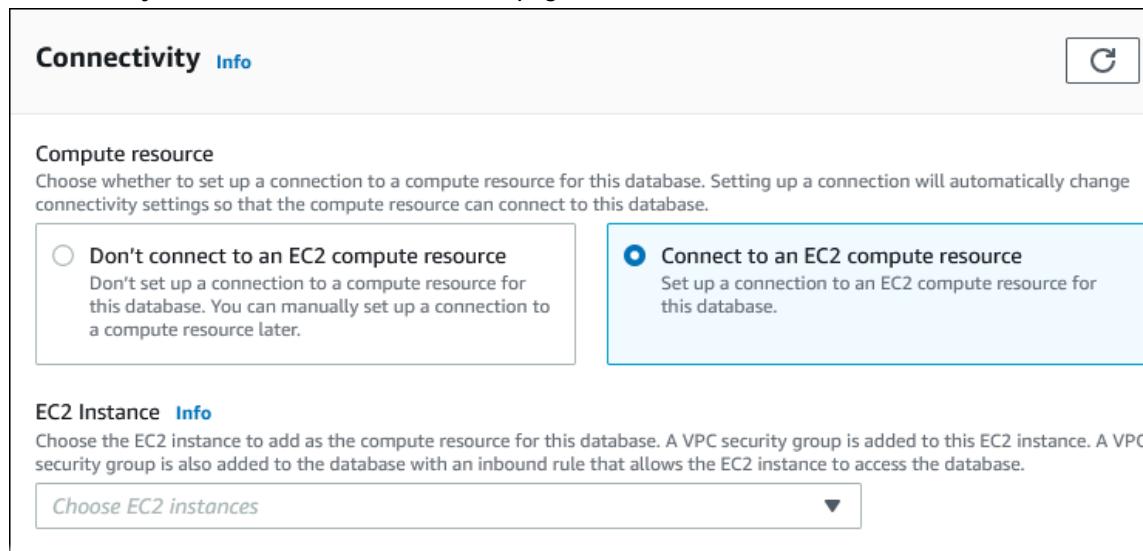
The following are requirements for connecting an EC2 instance with the DB cluster:

- The EC2 instance must exist in the AWS Region before you create the DB cluster.
If no EC2 instances exist in the AWS Region, the console provides a link to create one.
- The user who is creating the DB cluster must have permissions to perform the following operations:
 - `ec2:AssociateRouteTable`
 - `ec2:AuthorizeSecurityGroupEgress`
 - `ec2>CreateRouteTable`

- ec2:CreateSubnet
- ec2:CreateSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:ModifyNetworkInterfaceAttribute
- ec2:RevokeSecurityGroupEgress

Using this option creates a private DB cluster. The DB cluster uses a DB subnet group with only private subnets to restrict access to resources within the VPC.

To connect an EC2 instance to the DB cluster, choose **Connect to an EC2 compute resource** in the **Connectivity** section on the **Create database** page.



Connectivity [Info](#) [C](#)

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

EC2 Instance [Info](#)
Choose the EC2 instance to add as the compute resource for this database. A VPC security group is added to this EC2 instance. A VPC security group is also added to the database with an inbound rule that allows the EC2 instance to access the database.

[Choose EC2 instances](#) ▾

When you choose **Connect to an EC2 compute resource**, RDS sets the following options automatically. You can't change these settings unless you choose not to set up connectivity with an EC2 instance by choosing **Don't connect to an EC2 compute resource**.

Console option	Automatic setting
Virtual Private Cloud (VPC)	RDS sets the VPC to the one associated with the EC2 instance.
DB subnet group	<p>A DB subnet group with a private subnet in each Availability Zone in the AWS Region is required. In some cases, a DB subnet group that meets this requirement exists. If so, RDS uses the existing DB subnet group.</p> <p>In some cases, a DB subnet group that meets this requirement doesn't exist. In these cases, RDS uses an available private subnet in each Availability Zone to create a DB subnet group using the private subnets. If a private subnet isn't available in an Availability Zone, RDS creates a private subnet in the Availability Zone. RDS then creates the DB subnet group.</p> <p>When a private subnet is available, RDS uses the route table associated with it and adds any subnets it creates to this route table. When no private</p>

Console option	Automatic setting
	subnet is available, RDS creates a route table with no internet gateway access. RDS then adds the subnets that it creates to the route table.
Public access	RDS chooses No so that the DB cluster isn't publicly accessible. For security, it is a best practice to keep the database private and make sure it isn't accessible from the internet.
VPC security group (firewall)	RDS creates a new security group that is associated with the DB cluster. The security group is named <code>rds-ec2-n</code> , where <i>n</i> is a number. This security group includes an inbound rule with the EC2 VPC security group (firewall) as the source. This security group that is associated with the DB cluster allows the EC2 instance to access the DB cluster. RDS also creates a new security group that is associated with the EC2 instance. The security group is named <code>ec2-rds-n</code> , where <i>n</i> is a number. This security group includes an outbound rule with the VPC security group of the DB cluster as the source. This security group allows the EC2 instance to send traffic to the DB cluster. You can add another new security group by choosing Create new and typing the name of the new security group. You can add existing security groups by choosing Choose existing and selecting security groups to add.
Availability Zone	RDS chooses the Availability Zone of the EC2 instance for one DB instance in the Multi-AZ DB cluster deployment. RDS randomly chooses a different Availability Zone for both of the other DB instances. The writer DB instance is created in the same Availability Zone as the EC2 instance. There is the possibility of cross Availability Zone costs if a failover occurs and the writer DB instance is in a different Availability Zone.

For more information about these settings, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).

If you change these settings after the DB cluster is created, the changes might affect the connection between the EC2 instance and the DB cluster.

Configure the network manually

To connect to your DB cluster from resources other than EC2 instances in the same VPC, configure the network connections manually. If you use the AWS Management Console to create your Multi-AZ DB cluster, you can have Amazon RDS automatically create a VPC for you. Or you can use an existing VPC or create a new VPC for your Multi-AZ DB cluster. Your VPC must have at least one subnet in each of at least three Availability Zones for you to use it with a Multi-AZ DB cluster. For information on VPCs, see [Amazon VPCs and Amazon RDS \(p. 2103\)](#).

If you don't have a default VPC or you haven't created a VPC, and you don't plan to use the console, do the following:

- Create a VPC with at least one subnet in each of at least three of the Availability Zones in the AWS Region where you want to deploy your DB cluster. For more information, see [Working with a DB instance in a VPC \(p. 2104\)](#).
- Specify a VPC security group that authorizes connections to your DB cluster. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#) and [Controlling access with security groups \(p. 2085\)](#).

- Specify an RDS DB subnet group that defines at least three subnets in the VPC that can be used by the Multi-AZ DB cluster. For more information, see [Working with DB subnet groups \(p. 2104\)](#).

For information about limitations that apply to Multi-AZ DB clusters, see [Limitations for Multi-AZ DB clusters \(p. 136\)](#).

Additional prerequisites

Before you create your Multi-AZ DB cluster, consider the following additional prerequisites:

- To connect to AWS using AWS Identity and Access Management (IAM) credentials, your AWS account must have certain IAM policies. These grant the permissions required to perform Amazon RDS operations. For more information, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

If you use IAM to access the RDS console, first sign in to the AWS Management Console with your IAM user credentials. Then go to the RDS console at <https://console.aws.amazon.com/rds/>.

- To tailor the configuration parameters for your DB cluster, specify a DB cluster parameter group with the required parameter settings. For information about creating or modifying a DB cluster parameter group, see [Working with parameter groups for Multi-AZ DB clusters \(p. 133\)](#).
- Determine the TCP/IP port number to specify for your DB cluster. The firewalls at some companies block connections to the default ports. If your company firewall blocks the default port, choose another port for your DB cluster. All DB instances in a DB cluster use the same port.

Creating a DB cluster

You can create a Multi-AZ DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

Console

You can create a Multi-AZ DB cluster by choosing **Multi-AZ cluster** in the **Availability and durability** section.

To create a Multi-AZ DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you want to create the DB cluster.

For information about the AWS Regions that support Multi-AZ DB clusters, see [Limitations for Multi-AZ DB clusters \(p. 136\)](#).
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.

To create a Multi-AZ DB cluster, make sure that **Standard Create** is selected and **Easy Create** isn't.
5. In **Engine type**, choose **MySQL** or **PostgreSQL**.
6. For **Version**, choose the DB engine version.

For information about the DB engine versions that support Multi-AZ DB clusters, see [Limitations for Multi-AZ DB clusters \(p. 136\)](#).
7. In **Templates**, choose the appropriate template for your deployment.
8. In **Availability and durability**, choose **Multi-AZ cluster**.

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB cluster

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance

Creates a single DB instance with no standby DB instances.

9. In **DB cluster identifier**, enter the identifier for your DB cluster.
10. In **Master username**, enter your master user name, or keep the default setting.
11. Enter your master password:
 - a. In the **Settings** section, open **Credential Settings**.
 - b. If you want to specify a password, clear the **Auto generate a password** box if it is selected.
 - c. (Optional) Change the **Master username** value.
 - d. Enter the same password in **Master password** and **Confirm password**.
12. In **DB instance class**, choose a DB instance class.
13. (Optional) Set up a connection to a compute resource for this DB cluster.

You can configure connectivity between an Amazon EC2 instance and the new DB cluster during DB cluster creation. For more information, see [Configure automatic network connectivity with an EC2 instance \(p. 252\)](#).

14. For the remaining sections, specify your DB cluster settings. For information about each setting, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).
15. Choose **Create database**.

If you chose to use an automatically generated password, the **View credential details** button appears on the **Databases** page.

To view the master user name and password for the DB cluster, choose **View credential details**.

To connect to the DB cluster as the master user, use the user name and password that appear.

Important

You can't view the master user password again.

16. For **Databases**, choose the name of the new DB cluster.

On the RDS console, the details for the new DB cluster appear. The DB cluster has a status of **Creating** until the DB cluster is created and ready for use. When the state changes to **Available**, you can connect to the DB cluster. Depending on the DB cluster class and storage allocated, it can take several minutes for the new DB cluster to be available.

AWS CLI

Before you create a Multi-AZ DB cluster using the AWS CLI, make sure to fulfill the required prerequisites. These include creating a VPC and an RDS DB subnet group. For more information, see [DB cluster prerequisites \(p. 252\)](#).

To create a Multi-AZ DB cluster by using the AWS CLI, call the [create-db-cluster](#) command. Specify the `--db-cluster-identifier`. For the `--engine` option, specify either `mysql` or `postgres`.

For information about each option, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).

For information about the AWS Regions, DB engines, and DB engine versions that support Multi-AZ DB clusters, see [Limitations for Multi-AZ DB clusters \(p. 136\)](#).

The `create-db-cluster` command creates the writer DB instance for your DB cluster, and two reader DB instances. Each DB instance is in a different Availability Zone.

For example, the following command creates a MySQL 8.0 Multi-AZ DB cluster named `mysql-multi-az-db-cluster`.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-cluster \
--db-cluster-identifier mysql-multi-az-db-cluster \
--engine mysql \
--engine-version 8.0.28 \
--master-user-password password \
--master-username admin \
--port 3306 \
--backup-retention-period 1 \
--db-subnet-group-name default \
--allocated-storage 4000 \
--storage-type io1 \
--iops 10000 \
--db-cluster-instance-class db.r6gd.xlarge
```

For Windows:

```
aws rds create-db-cluster ^
--db-cluster-identifier mysql-multi-az-db-cluster ^
--engine mysql ^
--engine-version 8.0.28 ^
--master-user-password password ^
--master-username admin ^
--port 3306 ^
--backup-retention-period 1 ^
--db-subnet-group-name default ^
--allocated-storage 4000 ^
--storage-type io1 ^
--iops 10000 ^
--db-cluster-instance-class db.r6gd.xlarge
```

The following command creates a PostgreSQL 13.4 Multi-AZ DB cluster named `postgresql-multi-az-db-cluster`.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-cluster \
--db-cluster-identifier postgresql-multi-az-db-cluster \
--engine postgres \
--engine-version 13.4 \
--master-user-password password \
--master-username postgres \
--port 5432 \
--backup-retention-period 1 \
```

```
--db-subnet-group-name default \
--allocated-storage 4000 \
--storage-type io1 \
--iops 10000 \
--db-cluster-instance-class db.r6gd.xlarge
```

For Windows:

```
aws rds create-db-cluster ^
--db-cluster-identifier postgresql-multi-az-db-cluster ^
--engine postgres ^
--engine-version 13.4 ^
--master-user-password password ^
--master-username postgres ^
--port 5432 ^
--backup-retention-period 1 ^
--db-subnet-group-name default ^
--allocated-storage 4000 ^
--storage-type io1 ^
--iops 10000 ^
--db-cluster-instance-class db.r6gd.xlarge
```

RDS API

Before you can create a Multi-AZ DB cluster using the RDS API, make sure to fulfill the required prerequisites, such as creating a VPC and an RDS DB subnet group. For more information, see [DB cluster prerequisites \(p. 252\)](#).

To create a Multi-AZ DB cluster by using the RDS API, call the [CreateDBCluster](#) operation. Specify the `DBClusterIdentifier`. For the `Engine` parameter, specify either `mysql` or `postgresql`.

For information about each option, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).

The `CreateDBCluster` operation creates the writer DB instance for your DB cluster, and two reader DB instances. Each DB instance is in a different Availability Zone.

Settings for creating Multi-AZ DB clusters

For details about settings that you choose when you create a Multi-AZ DB cluster, see the following table. For more information about the AWS CLI options, see [create-db-cluster](#). For more information about the RDS API parameters, see [CreateDBCluster](#).

Console setting	Setting description	CLI option and RDS API parameter
Allocated storage	<p>The amount of storage to allocate for each DB instance in your DB cluster (in gibibyte).</p> <p>For more information, see Amazon RDS DB instance storage (p. 64).</p>	CLI option: <code>--allocated-storage</code> API parameter: <code>AllocatedStorage</code>
Auto minor version upgrade	<p>Enable auto minor version upgrade to have your DB cluster receive preferred minor DB engine version upgrades automatically when they become available. Amazon RDS performs automatic minor version upgrades in the maintenance window.</p>	CLI option: <code>--auto-minor-version-upgrade</code> <code>--no-auto-minor-version-upgrade</code> API parameter: <code>AutoMinorVersionUpgrade</code>

Console setting	Setting description	CLI option and RDS API parameter
		AutoMinorVersionUpgrade
Backup retention period	The number of days that you want automatic backups of your DB cluster to be retained. For a Multi-AZ DB cluster, this value must be set to 1 or greater. For more information, see Working with backups (p. 427) .	CLI option: --backup-retention-period API parameter: BackupRetentionPeriod
Backup window	The time period during which Amazon RDS automatically takes a backup of your DB cluster. Unless you have a specific time that you want to have your database backed up, use the default of No preference . For more information, see Working with backups (p. 427) .	CLI option: --preferred-backup-window API parameter: PreferredBackupWindow
Copy tags to snapshots	This option copies any DB cluster tags to a DB snapshot when you create a snapshot. For more information, see Tagging Amazon RDS resources (p. 392) .	CLI option: -copy-tags-to-snapshot -no-copy-tags-to-snapshot RDS API parameter: CopyTagsToSnapshot
Database authentication	For Multi-AZ DB clusters, only Password authentication is supported.	None because password authentication is the default.
Database port	The port that you want to access the DB cluster through. The default port is shown. The port can't be changed after the DB cluster is created. The firewalls at some companies block connections to the default ports. If your company firewall blocks the default port, enter another port for your DB cluster.	CLI option: --port RDS API parameter: Port
DB cluster identifier	The name for your DB cluster. Name your DB clusters in the same way that you name your on-premises servers. Your DB cluster identifier can contain up to 63 alphanumeric characters, and must be unique for your account in the AWS Region you chose.	CLI option: --db-cluster-identifier RDS API parameter: DBClusterIdentifier

Console setting	Setting description	CLI option and RDS API parameter
DB cluster instance class	<p>The compute and memory capacity of each DB instance in the Multi-AZ DB cluster, for example db.r6gd.xlarge.</p> <p>If possible, choose a DB instance class large enough that a typical query working set can be held in memory. When working sets are held in memory the system can avoid writing to disk, which improves performance.</p> <p>Currently, Multi-AZ DB clusters only support db.m6gd and db.r6gd DB instance classes. For more information about DB instance classes, see DB instance classes (p. 10).</p>	<p>CLI option: --db-cluster-instance-class</p> <p>RDS API parameter: DBClusterInstanceClass</p>
DB cluster parameter group	<p>The DB cluster parameter group that you want associated with the DB cluster.</p> <p>For more information, see Working with parameter groups for Multi-AZ DB clusters (p. 133).</p>	<p>CLI option: --db-cluster-parameter-group-name</p> <p>RDS API parameter: DBClusterParameterGroupName</p>
DB engine version	The version of database engine that you want to use.	<p>CLI option: --engine-version</p> <p>RDS API parameter: EngineVersion</p>
DB parameter group	<p>The DB instance parameter group that you want associated with the DB instances in the DB cluster.</p> <p>For more information, see Working with parameter groups for Multi-AZ DB clusters (p. 133).</p>	Not applicable. Amazon RDS associates each DB instance with the appropriate default parameter group.
DB subnet group	<p>A DB subnet group to associate with this DB cluster.</p> <p>For more information, see Working with DB subnet groups (p. 2104).</p>	<p>CLI option: --db-subnet-group-name</p> <p>RDS API parameter: DBSubnetGroupName</p>
Deletion protection	<p>Enable deletion protection to prevent your DB cluster from being deleted. If you create a production DB cluster with the console, deletion protection is turned on by default.</p> <p>For more information, see Deleting a DB instance (p. 421).</p>	<p>CLI option: --deletion-protection --no-deletion-protection</p> <p>RDS API parameter: DeletionProtection</p>

Console setting	Setting description	CLI option and RDS API parameter
Encryption	<p>Enable Encryption to turn on encryption at rest for this DB cluster.</p> <p>Encryption is turned on by default for Multi-AZ DB clusters.</p> <p>For more information, see Encrypting Amazon RDS resources (p. 2000).</p>	<p>CLI options:</p> <ul style="list-style-type: none"> --kms-key-id --storage-encrypted --no-storage-encrypted <p>RDS API parameters:</p> <ul style="list-style-type: none"> KmsKeyId StorageEncrypted
Enhanced Monitoring	<p>Enable enhanced monitoring to turn on metrics gathering in real time for the operating system that your DB cluster runs on.</p> <p>For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600).</p>	<p>CLI options:</p> <ul style="list-style-type: none"> --monitoring-interval --monitoring-role-arn <p>RDS API parameters:</p> <ul style="list-style-type: none"> MonitoringInterval MonitoringRoleArn
Initial database name	<p>The name for the database on your DB cluster. If you don't provide a name, Amazon RDS doesn't create a database on the DB cluster for MySQL. However, it does create a database on the DB cluster for PostgreSQL. The name can't be a word reserved by the database engine. It has other constraints depending on the DB engine.</p> <p>MySQL:</p> <ul style="list-style-type: none"> • It must contain 1–64 alphanumeric characters. <p>PostgreSQL:</p> <ul style="list-style-type: none"> • It must contain 1–63 alphanumeric characters. • It must begin with a letter or an underscore. Subsequent characters can be letters, underscores, or digits (0–9). • The initial database name is <code>postgres</code>. 	<p>CLI option:</p> <ul style="list-style-type: none"> --database-name <p>RDS API parameter:</p> <ul style="list-style-type: none"> DatabaseName
Log exports	<p>The types of database log files to publish to Amazon CloudWatch Logs.</p> <p>For more information, see Publishing database logs to Amazon CloudWatch Logs (p. 683).</p>	<p>CLI option:</p> <ul style="list-style-type: none"> -enable-cloudwatch-logs-exports <p>RDS API parameter:</p> <ul style="list-style-type: none"> EnableCloudwatchLogsExports

Console setting	Setting description	CLI option and RDS API parameter
Maintenance window	<p>The 30-minute window in which pending modifications to your DB cluster are applied. If the time period doesn't matter, choose No preference.</p> <p>For more information, see The Amazon RDS maintenance window (p. 354).</p>	CLI option: --preferred-maintenance-window RDS API parameter: PreferredMaintenanceWindow
Master password	<p>The password for your master user account.</p>	CLI option: --master-user-password RDS API parameter: MasterUserPassword
Master username	<p>The name that you use as the master user name to log on to your DB cluster with all database privileges.</p> <ul style="list-style-type: none"> It can contain 1–16 alphanumeric characters and underscores. Its first character must be a letter. It can't be a word reserved by the database engine. <p>You can't change the master user name after the Multi-AZ DB cluster is created.</p> <p>For more information on privileges granted to the master user, see Master user account privileges (p. 2087).</p>	CLI option: --master-username RDS API parameter: MasterUsername

Console setting	Setting description	CLI option and RDS API parameter
Performance Insights	<p>Enable Performance Insights to monitor your DB cluster load so that you can analyze and troubleshoot your database performance.</p> <p>Choose a retention period to determine how much Performance Insights data history to keep. The retention setting in the free tier is Default (7 days). To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see Pricing and data retention for Performance Insights (p. 548).</p> <p>Choose a master key to use to protect the key used to encrypt this database volume. Choose from the master keys in your account, or enter the key from a different account.</p> <p>For more information, see Monitoring DB load with Performance Insights on Amazon RDS (p. 543).</p>	<p>CLI options:</p> <pre>--enable-performance-insights --no-enable-performance-insights --performance-insights-retention-period --performance-insights-kms-key-id</pre> <p>RDS API parameters:</p> <pre>EnablePerformanceInsights PerformanceInsightsRetentionPeriod PerformanceInsightsKMSKeyId</pre>
Provisioned IOPS	<p>The amount of Provisioned IOPS (input/output operations per second) to be initially allocated for the DB cluster. This setting is available only if Provisioned IOPS (io1) is selected as the storage type.</p> <p>For more information, see Provisioned IOPS SSD storage (p. 66).</p>	<p>CLI option:</p> <pre>--iops</pre> <p>RDS API parameter:</p> <pre>Iops</pre>

Console setting	Setting description	CLI option and RDS API parameter
Public access	<p>Publicly accessible to give the DB cluster a public IP address, meaning that it's accessible outside the VPC. To be publicly accessible, the DB cluster also has to be in a public subnet in the VPC.</p> <p>Not publicly accessible to make the DB cluster accessible only from inside the VPC.</p> <p>For more information, see Hiding a DB instance in a VPC from the internet (p. 2109).</p> <p>To connect to a DB cluster from outside of its VPC, the DB cluster must be publicly accessible. Also, access must be granted using the inbound rules of the DB cluster's security group, and other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 2141).</p> <p>If your DB cluster isn't publicly accessible, you can use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 2015).</p>	<p>CLI option:</p> <pre>--publicly-accessible</pre> <pre>--no-publicly-accessible</pre> <p>RDS API parameter:</p> <pre>PubliclyAccessible</pre>
Storage type	<p>The storage type for your DB cluster.</p> <p>Only Provisioned IOPS (io1) storage is supported. General Purpose (gp2) and General Purpose (gp3) storage aren't supported.</p> <p>For more information, see Amazon RDS storage types (p. 64).</p>	<p>CLI option:</p> <pre>--storage-type</pre> <p>RDS API parameter:</p> <pre>StorageType</pre>
Virtual Private Cloud (VPC)	<p>A VPC based on the Amazon VPC service to associate with this DB cluster.</p> <p>For more information, see Amazon VPC VPCs and Amazon RDS (p. 2103).</p>	For the CLI and API, you specify the VPC security group IDs.
VPC security group (firewall)	<p>The security groups to associate with the DB cluster.</p> <p>For more information, see Overview of VPC security groups (p. 2085).</p>	<p>CLI option:</p> <pre>--vpc-security-group-ids</pre> <p>RDS API parameter:</p> <pre>VpcSecurityGroupIds</pre>

Settings that don't apply when creating Multi-AZ DB clusters

The following settings in the AWS CLI command [create-db-cluster](#) and the RDS API operation [CreateDBCluster](#) don't apply to Multi-AZ DB clusters.

You also can't specify these settings for Multi-AZ DB clusters in the console.

AWS CLI setting	RDS API setting
--availability-zones	AvailabilityZones
--backtrack-window	BacktrackWindow
--character-set-name	CharacterSetName
--domain	Domain
--domain-iam-role-name	DomainIAMRoleName
--enable-global-write-forwarding --no-enable-global-write-forwarding	EnableGlobalWriteForwarding
--enable-http-endpoint --no-enable-http-endpoint	EnableHttpEndpoint
--enable-iam-database-authentication --no-enable-iam-database-authentication	EnableIAMDATABASEAuthentication
--global-cluster-identifier	GlobalClusterIdentifier
--option-group-name	OptionGroupName
--pre-signed-url	PreSignedUrl
--replication-source-identifier	ReplicationSourceIdentifier
--scaling-configuration	ScalingConfiguration

Creating Amazon RDS resources with AWS CloudFormation

Amazon RDS is integrated with AWS CloudFormation, a service that helps you to model and set up your AWS resources so that you can spend less time creating and managing your resources and infrastructure. You create a template that describes all the AWS resources that you want (such as DB instances and DB parameter groups), and AWS CloudFormation provisions and configures those resources for you.

When you use AWS CloudFormation, you can reuse your template to set up your RDS resources consistently and repeatedly. Describe your resources once, and then provision the same resources over and over in multiple AWS accounts and Regions.

RDS and AWS CloudFormation templates

To provision and configure resources for RDS and related services, you must understand [AWS CloudFormation templates](#). Templates are formatted text files in JSON or YAML. These templates describe the resources that you want to provision in your AWS CloudFormation stacks. If you're unfamiliar with JSON or YAML, you can use AWS CloudFormation Designer to help you get started with AWS CloudFormation templates. For more information, see [What is AWS CloudFormation Designer?](#) in the [AWS CloudFormation User Guide](#).

RDS supports creating resources in AWS CloudFormation. For more information, including examples of JSON and YAML templates for these resources, see the [RDS resource type reference](#) in the [AWS CloudFormation User Guide](#).

Learn more about AWS CloudFormation

To learn more about AWS CloudFormation, see the following resources:

- [AWS CloudFormation](#)
- [AWS CloudFormation User Guide](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Command Line Interface User Guide](#)

Connecting to an Amazon RDS DB instance

Before you can connect to a DB instance, you must create the DB instance. For information, see [Creating an Amazon RDS DB instance \(p. 230\)](#). After Amazon RDS provisions your DB instance, use any standard client application or utility for your DB engine to connect to the DB instance. In the connection string, specify the DNS address from the DB instance endpoint as the host parameter. Also, specify the port number from the DB instance endpoint as the port parameter.

Topics

- [Finding the connection information for an Amazon RDS DB instance \(p. 267\)](#)
- [Database authentication options \(p. 270\)](#)
- [Encrypted connections \(p. 271\)](#)
- [Scenarios for accessing a DB instance in a VPC \(p. 271\)](#)
- [Connecting to a DB instance that is running a specific DB engine \(p. 271\)](#)
- [Managing connections with RDS Proxy \(p. 272\)](#)

Finding the connection information for an Amazon RDS DB instance

The connection information for a DB instance includes its endpoint, port, and a valid database user, such as the master user. For example, for a MySQL DB instance, suppose that the endpoint value is `mydb.123456789012.us-east-1.rds.amazonaws.com`. In this case, the port value is 3306, and the database user is `admin`. Given this information, you specify the following values in a connection string:

- For host or host name or DNS name, specify `mydb.123456789012.us-east-1.rds.amazonaws.com`.
- For port, specify 3306.
- For user, specify `admin`.

The endpoint is unique for each DB instance, and the values of the port and user can vary. The following list shows the most common port for each DB engine:

- MariaDB – 3306
- Microsoft SQL Server – 1433
- MySQL – 3306
- Oracle – 1521
- PostgreSQL – 5432

To connect to a DB instance, use any client for a DB engine. For example, you might use the `mysql` utility to connect to a MariaDB or MySQL DB instance. You might use Microsoft SQL Server Management Studio to connect to a SQL Server DB instance. You might use Oracle SQL Developer to connect to an Oracle DB instance. Similarly, you might use the `psql` command line utility to connect to a PostgreSQL DB instance.

To find the connection information for a DB instance, use the AWS Management Console. You can also use the AWS Command Line Interface (AWS CLI) `describe-db-instances` command or the RDS API `DescribeDBInstances` operation.

Console

To find the connection information for a DB instance in the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases** to display a list of your DB instances.
3. Choose the name of the DB instance to display its details.
4. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the AWS RDS console interface. At the top, the navigation path is "RDS > Databases > mydb". Below this, the database name "mydb" is displayed in large text. A "Summary" section provides basic information: DB identifier (mydb), Role (Instance), CPU usage (2.33%), and Current activity (0 Connections). Below the summary is a tab bar with "Connectivity & security" (highlighted in orange), "Monitoring", "Logs & events", and "Configuration". The "Connectivity & security" section displays the endpoint and port details, which are circled in red. The endpoint is listed as "mydb. [REDACTED].us-east-1.rds.amazonaws.com" and the port is listed as "3306". To the right of the main content area, there is a vertical sidebar with network, availability zone, VPC, and subnet information.

Network	Available	VPC	Subnet
us-east-1	us-eas	vpc-65	default

5. If you need to find the master user name, choose the **Configuration** tab and view the **Master username** value.

AWS CLI

To find the connection information for a DB instance by using the AWS CLI, call the [describe-db-instances](#) command. In the call, query for the DB instance ID, endpoint, port, and master user name.

For Linux, macOS, or Unix:

```
aws rds describe-db-instances \
--query "[].{DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername}"
```

For Windows:

```
aws rds describe-db-instances ^
--query "[].{DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername}"
```

Your output should be similar to the following.

```
[  
  [  
    "mydb",  
    "mydb.123456789012.us-east-1.rds.amazonaws.com",  
    3306,  
    "admin"  
  ],  
  [  
    "myoracledb",  
    "myoracledb.123456789012.us-east-1.rds.amazonaws.com",  
    1521,  
    "dbadmin"  
  ],  
  [  
    "mypostgresql",  
    "mypostgresql.123456789012.us-east-1.rds.amazonaws.com",  
    5432,  
    "postgresadmin"  
  ]  
]
```

RDS API

To find the connection information for a DB instance by using the Amazon RDS API, call the [DescribeDBInstances](#) operation. In the output, find the values for the endpoint address, endpoint port, and master user name.

Database authentication options

Amazon RDS supports the following ways to authenticate database users:

- **Password authentication** – Your DB instance performs all administration of user accounts. You create users and specify passwords with SQL statements. The SQL statements you can use depend on your DB engine.
- **AWS Identity and Access Management (IAM) database authentication** – You don't need to use a password when you connect to a DB instance. Instead, you use an authentication token.
- **Kerberos authentication** – You use external authentication of database users using Kerberos and Microsoft Active Directory. Kerberos is a network authentication protocol that uses tickets and symmetric-key cryptography to eliminate the need to transmit passwords over the network. Kerberos has been built into Active Directory and is designed to authenticate users to network resources, such as databases.

IAM database authentication and Kerberos authentication are available only for specific DB engines and versions.

For more information, see [Database authentication with Amazon RDS \(p. 1998\)](#).

Encrypted connections

You can use Secure Socket Layer (SSL) or Transport Layer Security (TLS) from your application to encrypt a connection to a DB instance. Each DB engine has its own process for implementing SSL/TLS. For more information, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

Scenarios for accessing a DB instance in a VPC

Using Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources, such as Amazon RDS DB instances, into a virtual private cloud (VPC). When you use Amazon VPC, you have control over your virtual networking environment. You can choose your own IP address range, create subnets, and configure routing and access control lists.

A VPC security group controls access to DB instances inside a VPC. Each VPC security group rule enables a specific source to access a DB instance in a VPC that is associated with that VPC security group. The source can be a range of addresses (for example, 203.0.113.0/24), or another VPC security group. By specifying a VPC security group as the source, you allow incoming traffic from all instances (typically application servers) that use the source VPC security group.

Before attempting to connect to your DB instance, configure your VPC for your use case. The following are common scenarios for accessing a DB instance in a VPC:

- **A DB instance in a VPC accessed by an Amazon EC2 instance in the same VPC** – A common use of a DB instance in a VPC is to share data with an application server that is running in an EC2 instance in the same VPC. The EC2 instance might run a web server with an application that interacts with the DB instance.
- **A DB instance in a VPC accessed by an EC2 instance in a different VPC** – In some cases, your DB instance is in a different VPC from the EC2 instance that you're using to access it. If so, you can use VPC peering to access the DB instance.
- **A DB instance in a VPC accessed by a client application through the internet** – To access a DB instance in a VPC from a client application through the internet, you configure a VPC with a single public subnet. You also configure an internet gateway to enable communication over the internet.

To connect to a DB instance from outside of its VPC, the DB instance must be publicly accessible. Also, access must be granted using the inbound rules of the DB instance's security group, and other requirements must be met. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

- **A DB instance in a VPC accessed by a private network** – If your DB instance isn't publicly accessible, you can use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network.

For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

Connecting to a DB instance that is running a specific DB engine

For information about connecting to a DB instance that is running a specific DB engine, follow the instructions for your DB engine:

- [Connecting to a DB instance running the MariaDB database engine \(p. 986\)](#)
- [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#)

- [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#)
- [Connecting to your Oracle DB instance \(p. 1488\)](#)
- [Connecting to a DB instance running the PostgreSQL database engine \(p. 1809\)](#)

Managing connections with RDS Proxy

You can also use Amazon RDS Proxy to manage connections to RDS for MariaDB, RDS for Microsoft SQL Server, RDS for MySQL, and RDS for PostgreSQL DB instances. RDS Proxy allows applications to pool and share database connections to improve scalability. For more information, see [Using Amazon RDS Proxy \(p. 921\)](#).

Working with option groups

Some DB engines offer additional features that make it easier to manage data and databases, and to provide additional security for your database. Amazon RDS uses option groups to enable and configure these features. An *option group* can specify features, called options, that are available for a particular Amazon RDS DB instance. Options can have settings that specify how the option works. When you associate a DB instance with an option group, the specified options and option settings are enabled for that DB instance.

Amazon RDS supports options for the following database engines:

Database engine	Relevant documentation
MariaDB	Options for MariaDB database engine (p. 1040)
Microsoft SQL Server	Options for the Microsoft SQL Server database engine (p. 1203)
MySQL	Options for MySQL DB instances (p. 1416)
Oracle	Adding options to Oracle DB instances (p. 1646)
PostgreSQL	PostgreSQL does not use options and option groups. PostgreSQL uses extensions and modules to provide additional features. For more information, see Supported PostgreSQL extension versions (p. 1807) .

Option groups overview

Amazon RDS provides an empty default option group for each new DB instance. You can't modify or delete this default option group, but any new option group that you create derives its settings from the default option group. To apply an option to a DB instance, you must do the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add one or more options to the option group.
3. Associate the option group with the DB instance.

To associate an option group with a DB instance, modify the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Both DB instances and DB snapshots can be associated with an option group. In some cases, you might restore from a DB snapshot or perform a point-in-time restore for a DB instance. In these cases, the option group associated with the DB snapshot or DB instance is, by default, associated with the restored DB instance. You can associate a different option group with a restored DB instance. However, the new option group must contain any persistent or permanent options that were included in the original option group. Persistent and permanent options are described following.

Options require additional memory to run on a DB instance. Thus, you might need to launch a larger instance to use them, depending on your current use of your DB instance. For example, Oracle Enterprise Manager Database Control uses about 300 MB of RAM. If you enable this option for a small DB instance, you might encounter performance problems or out-of-memory errors.

Persistent and permanent options

Two types of options, persistent and permanent, require special consideration when you add them to an option group.

Persistent options can't be removed from an option group while DB instances are associated with the option group. An example of a persistent option is the TDE option for Microsoft SQL Server transparent data encryption (TDE). You must disassociate all DB instances from the option group before a persistent option can be removed from the option group. In some cases, you might restore or perform a point-in-time restore from a DB snapshot. In these cases, if the option group associated with that DB snapshot contains a persistent option, you can only associate the restored DB instance with that option group.

Permanent options, such as the TDE option for Oracle Advanced Security TDE, can never be removed from an option group. You can change the option group of a DB instance that is using the permanent option. However, the option group associated with the DB instance must include the same permanent option. In some cases, you might restore or perform a point-in-time restore from a DB snapshot. In these cases, if the option group associated with that DB snapshot contains a permanent option, you can only associate the restored DB instance with an option group with that permanent option.

For Oracle DB instances, you can copy shared DB snapshots that have the options Timezone or OLS (or both). To do so, specify a target option group that includes these options when you copy the DB snapshot. The OLS option is permanent and persistent only for Oracle DB instances running Oracle version 12.2 or higher. For more information about these options, see [Oracle time zone \(p. 1742\)](#) and [Oracle Label Security \(p. 1703\)](#).

VPC considerations

The option group associated with the DB instance is linked to the DB instance's VPC. This means that you can't use the option group assigned to a DB instance if you try to restore the instance to a different VPC. If you restore a DB instance to a different VPC, you can do one of the following:

- Assign the default option group to the DB instance.
- Assign an option group that is linked to that VPC.
- Create a new option group and assign it to the DB instance.

With persistent or permanent options, such as Oracle TDE, you must create a new option group. This option group must include the persistent or permanent option when restoring a DB instance into a different VPC.

Option settings control the behavior of an option. For example, the Oracle Advanced Security option NATIVE_NETWORK_ENCRYPTION has a setting that you can use to specify the encryption algorithm for network traffic to and from the DB instance. Some options settings are optimized for use with Amazon RDS and cannot be changed.

Mutually exclusive options

Some options are mutually exclusive. You can use one or the other, but not both at the same time. The following options are mutually exclusive:

- [Oracle Enterprise Manager Database Express \(p. 1689\)](#) and [Oracle Management Agent for Enterprise Manager Cloud Control \(p. 1693\)](#).
- [Oracle native network encryption \(p. 1711\)](#) and [Oracle Secure Sockets Layer \(p. 1722\)](#).

Creating an option group

You can create a new option group that derives its settings from the default option group. You then add one or more options to the new option group. Or, if you already have an existing option group, you can copy that option group with all of its options to a new option group. For more information, see [Copying an option group \(p. 276\)](#).

After you create a new option group, it has no options. To learn how to add options to the option group, see [Adding an option to an option group \(p. 277\)](#). After you have added the options you want, you can then associate the option group with a DB instance. This way, the options become available on the DB instance. For information about associating an option group with a DB instance, see the documentation for your engine in [Working with option groups \(p. 273\)](#).

Console

One way of creating an option group is by using the AWS Management Console.

To create a new option group by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** window, do the following:
 - a. For **Name**, type a name for the option group that is unique within your AWS account. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, type a brief description of the option group. The description is used for display purposes.
 - c. For **Engine**, choose the DB engine that you want.
 - d. For **Major engine version**, choose the major version of the DB engine that you want.
5. To continue, choose **Create**. To cancel the operation instead, choose **Cancel**.

AWS CLI

To create an option group, use the AWS CLI `create-option-group` command with the following required parameters.

- `--option-group-name`
- `--engine-name`
- `--major-engine-version`
- `--option-group-description`

Example

The following example creates an option group named `testoptiongroup`, which is associated with the Oracle Enterprise Edition DB engine. The description is enclosed in quotation marks.

For Linux, macOS, or Unix:

```
aws rds create-option-group \
--option-group-name testoptiongroup \
--engine-name oracle-ee \
--major-engine-version 12.1 \
--option-group-description "Test option group"
```

For Windows:

```
aws rds create-option-group \
--option-group-name <i>testoptiongroup</i> \
--engine-name <i>oracle-ee</i> \
--major-engine-version <i>12.1</i> \
--option-group-description "<i>Test option group</i>"
```

```
aws rds create-option-group ^
--option-group-name testoptiongroup ^
--engine-name oracle-ee ^
--major-engine-version 12.1 ^
--option-group-description "Test option group"
```

RDS API

To create an option group, call the Amazon RDS API [CreateOptionGroup](#) operation. Include the following parameters:

- OptionGroupName
- EngineName
- MajorEngineVersion
- OptionGroupDescription

Copying an option group

You can use the AWS CLI or the Amazon RDS API copy an option group. Copying an option group can be convenient. An example is when you have an existing option group and want to include most of its custom parameters and values in a new option group. You can also make a copy of an option group that you use in production and then modify the copy to test other option settings.

Note

Currently, you can't copy an option group to a different AWS Region.

AWS CLI

To copy an option group, use the AWS CLI [copy-option-group](#) command. Include the following required options:

- --source-option-group-identifier
- --target-option-group-identifier
- --target-option-group-description

Example

The following example creates an option group named new-option-group, which is a local copy of the option group my-option-group.

For Linux, macOS, or Unix:

```
aws rds copy-option-group \
--source-option-group-identifier my-option-group \
--target-option-group-identifier new-option-group \
--target-option-group-description "My new option group"
```

For Windows:

```
aws rds copy-option-group ^
--source-option-group-identifier my-option-group ^
--target-option-group-identifier new-option-group ^
--target-option-group-description "My new option group"
```

RDS API

To copy an option group, call the Amazon RDS API [CopyOptionGroup](#) operation. Include the following required parameters.

- `SourceOptionGroupIdentifier`
- `TargetOptionGroupIdentifier`
- `TargetOptionGroupDescription`

Adding an option to an option group

You can add an option to an existing option group. After you have added the options you want, you can then associate the option group with a DB instance so that the options become available on the DB instance. For information about associating an option group with a DB instance, see the documentation for your specific DB engine listed at [Working with option groups \(p. 273\)](#).

Option group changes must be applied immediately in two cases:

- When you add an option that adds or updates a port value, such as the OEM option.
- When you add or remove an option group with an option that includes a port value.

In these cases, choose the **Apply Immediately** option in the console. Or you can include the `--apply-immediately` option when using the AWS CLI or set the `ApplyImmediately` parameter to true when using the Amazon RDS API. Options that don't include port values can be applied immediately, or can be applied during the next maintenance window for the DB instance.

Note

If you specify a security group as a value for an option in an option group, manage the security group by modifying the option group. You can't change or remove this security group by modifying a DB instance. Also, the security group doesn't appear in the DB instance details in the AWS Management Console or in the output for the AWS CLI command `describe-db-instances`.

Console

You can use the AWS Management Console to add an option to an option group.

To add an option to an option group by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group that you want to modify, and then choose **Add option**.

Option groups (9)		
<input type="text"/> Filter subnet groups		
	Name	Description
<input type="checkbox"/>	carpcmysql	carpcmysql
<input checked="" type="checkbox"/>	carpcoracle	carpcoracle
<input type="checkbox"/>	default:mysql-5-5	Default option group for mysql 5.5
<input type="checkbox"/>	default:mysql-5-6	Default option group for mysql 5.6
<input type="checkbox"/>	default:mysql-5-7	Default option group for mysql 5.7

4. In the **Add option** window, do the following:
 - a. Choose the option that you want to add. You might need to provide additional values, depending on the option that you select. For example, when you choose the OEM option, you must also type a port value and specify a security group.
 - b. To enable the option on all associated DB instances as soon as you add it, for **Apply Immediately**, choose **Yes**. If you choose **No** (the default), the option is enabled for each associated DB instance during its next maintenance window.

Add Option

Option details

Option group name
carpcoracle

Option
Name of Option you want to add to this group
OEM

Port
The port number, if applicable, to use when connecting to the Option
1158

Security Groups
A list of VPC or DB Security Groups for which this Option is enabled
Choose security groups
default X

Apply Immediately [info](#)
 Yes
 No

[Cancel](#) [Add Option](#)

- When the settings are as you want them, choose **Add option**.

AWS CLI

To add an option to an option group, run the AWS CLI [add-option-to-option-group](#) command with the option that you want to add. To enable the new option immediately on all associated DB instances, include the `--apply-immediately` parameter. By default, the option is enabled for each associated DB instance during its next maintenance window. Include the following required parameter:

- `--option-group-name`

Example

The following example adds the Oracle Enterprise Manager Database Control (OEM) option to an option group named `testoptiongroup` and immediately enables it. Even if you use the default security group, you must specify that security group.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
```

```
--option-group-name testoptiongroup \
--options OptionName=OEM,Port=5500,DBSecurityGroupMemberships=default \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name testoptiongroup ^
--options OptionName=OEM,Port=5500,DBSecurityGroupMemberships=default ^
--apply-immediately
```

Command output is similar to the following:

```
OPTIONGROUP  False  oracle-ee  12.1  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
  Test Option Group  testoptiongroup default
OPTIONS Oracle 12c EM Express  OEM      False    False   5500
DBSECURITYGROUPEMEMBERSHIPS  default authorized
```

Example

The following example adds the Oracle OEM option to an option group. It also specifies a custom port and a pair of Amazon EC2 VPC security groups to use for that port.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name testoptiongroup \
--options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2" \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name testoptiongroup ^
--options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2" ^
--apply-immediately
```

Command output is similar to the following:

```
OPTIONGROUP  False  oracle-ee  12.1  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
  Test Option Group  testoptiongroup vpc-test
OPTIONS Oracle 12c EM Express  OEM      False    False   5500
VPCSECURITYGROUPEMEMBERSHIPS  active  sg-test1
VPCSECURITYGROUPEMEMBERSHIPS  active  sg-test2
```

Example

The following example adds the Oracle option NATIVE_NETWORK_ENCRYPTION to an option group and specifies the option settings. If no option settings are specified, default values are used.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name testoptiongroup \
--options '[{"OptionSettings": [{"Name": "SQLNET.ENCRYPTION_SERVER", "Value": "REQUIRED"}, {"Name": "SQLNET.ENCRYPTION_TYPES_SERVER", "Value": "AES256,AES192,DES"}]}, {"OptionName": "NATIVE_NETWORK_ENCRYPTION", "Value": "AES256,AES192,DES"}]' \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name testoptiongroup ^
--options "OptionSettings=[{"Name": "SQLNET.ENCRYPTION_SERVER", "Value": "REQUIRED"}, {"Name": "SQLNET.ENCRYPTION_TYPES_SERVER", "Value": "AES256\,AES192\,DES"}], "OptionName": "NATIVE_NETWORK_ENCRYPTION", ^
--apply-immediately
```

Command output is similar to the following:

```
OPTIONGROUP False oracle-ee 12.1 arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
Test Option Group testoptiongroup
OPTIONS Oracle Advanced Security - Native Network Encryption NATIVE_NETWORK_ENCRYPTION
    False False
OPTIONSETTINGS
    RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40
        STATIC STRING
    RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40      Specifies
        list of encryption algorithms in order of intended use
    True True SQLNET.ENCRYPTION_TYPES_SERVER AES256,AES192,DES
OPTIONSETTINGS ACCEPTED,REJECTED,REQUESTED,REQUIRED STATIC STRING REQUESTED
        Specifies the desired encryption behavior False True SQLNET.ENCRYPTION_SERVER
        REQUIRED
OPTIONSETTINGS SHA1,MD5 STATIC STRING SHA1,MD5 Specifies list of checksumming
        algorithms in order of intended use True True SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
        SHA1,MD5
```

RDS API

To add an option to an option group using the Amazon RDS API, call the [ModifyOptionGroup](#) operation with the option that you want to add. To enable the new option immediately on all associated DB instances, include the `ApplyImmediately` parameter and set it to `true`. By default, the option is enabled for each associated DB instance during its next maintenance window. Include the following required parameter:

- `OptionGroupName`

Listing the options and option settings for an option group

You can list all the options and option settings for an option group.

Console

You can use the AWS Management Console to list all of the options and option settings for an option group.

To list the options and option settings for an option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the name of the option group to display its details. The options and option settings in the option group are listed.

AWS CLI

To list the options and option settings for an option group, use the AWS CLI `describe-option-groups` command. Specify the name of the option group whose options and settings you want to view. If you don't specify an option group name, all option groups are described.

Example

The following example lists the options and option settings for all option groups.

```
aws rds describe-option-groups
```

Example

The following example lists the options and option settings for an option group named `testoptiongroup`.

```
aws rds describe-option-groups --option-group-name testoptiongroup
```

RDS API

To list the options and option settings for an option group, use the Amazon RDS API `DescribeOptionGroups` operation. Specify the name of the option group whose options and settings you want to view. If you don't specify an option group name, all option groups are described.

Modifying an option setting

After you have added an option that has modifiable option settings, you can modify the settings at any time. If you change options or option settings in an option group, those changes are applied to all DB instances that are associated with that option group. For more information on what settings are available for the various options, see the documentation for your engine in [Working with option groups \(p. 273\)](#).

Option group changes must be applied immediately in two cases:

- When you add an option that adds or updates a port value, such as the OEM option.
- When you add or remove an option group with an option that includes a port value.

In these cases, choose the **Apply Immediately** option in the console. Or you can include the `--apply-immediately` option when using the AWS CLI or set the `ApplyImmediately` parameter to `true` when

using the RDS API. Options that don't include port values can be applied immediately, or can be applied during the next maintenance window for the DB instance.

Note

If you specify a security group as a value for an option in an option group, you manage the security group by modifying the option group. You can't change or remove this security group by modifying a DB instance. Also, the security group doesn't appear in the DB instance details in the AWS Management Console or in the output for the AWS CLI command `describe-db-instances`.

Console

You can use the AWS Management Console to modify an option setting.

To modify an option setting by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Select the option group whose option that you want to modify, and then choose **Modify option**.
4. In the **Modify option** window, from **Installed Options**, choose the option whose setting you want to modify. Make the changes that you want.
5. To enable the option as soon as you add it, for **Apply Immediately**, choose **Yes**. If you choose **No** (the default), the option is enabled for each associated DB instance during its next maintenance window.
6. When the settings are as you want them, choose **Modify Option**.

AWS CLI

To modify an option setting, use the AWS CLI `add-option-to-option-group` command with the option group and option that you want to modify. By default, the option is enabled for each associated DB instance during its next maintenance window. To apply the change immediately to all associated DB instances, include the `--apply-immediately` parameter. To modify an option setting, use the `--settings` argument.

Example

The following example modifies the port that the Oracle Enterprise Manager Database Control (OEM) uses in an option group named `testoptiongroup` and immediately applies the change.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name testoptiongroup \
--options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name testoptiongroup ^
--options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default ^
--apply-immediately
```

Command output is similar to the following:

```
OPTIONGROUP  False  oracle-ee  12.1  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
  Test Option Group  testoptiongroup
OPTIONS Oracle 12c EM Express  OEM  False  False  5432
DBSECURITYGROUPMEMBERSHIPS  default  authorized
```

Example

The following example modifies the Oracle option NATIVE_NETWORK_ENCRYPTION and changes the option settings.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name testoptiongroup \
--options '[{"OptionSettings": [{"Name": "SQLNET.ENCRYPTION_SERVER", "Value": "REQUIRED"}, {"Name": "SQLNET.ENCRYPTION_TYPES_SERVER", "Value": "AES256,AES192,DES,RC4_256"}]}, {"OptionName": "NATIVE_NETWORK_ENCRYPTION", "Value": "AES256,AES192,DES,RC4_256"}]' \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name testoptiongroup ^
--options "OptionSettings=[{"Name": "SQLNET.ENCRYPTION_SERVER", "Value": "REQUIRED"}, {"Name": "SQLNET.ENCRYPTION_TYPES_SERVER", "Value": "AES256\,AES192\,DES\,RC4_256"}], "OptionName": "NATIVE_NETWORK_ENCRYPTION" ^
--apply-immediately
```

Command output is similar to the following:

```
OPTIONGROUP  False  oracle-ee  12.1  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
  Test Option Group  testoptiongroup
OPTIONS Oracle Advanced Security - Native Network Encryption  NATIVE_NETWORK_ENCRYPTION
  False  False
OPTIONSETTINGS
  RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40  STATIC
  STRING
    RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40
    Specifies list of encryption algorithms in order of intended use
      True  True  SQLNET.ENCRYPTION_TYPES_SERVER  AES256,AES192,DES,RC4_256
OPTIONSETTINGS  ACCEPTED,REJECTED,REQUESTED,REQUIRED  STATIC  STRING  REQUESTED
  Specifies the desired encryption behavior  False  True  SQLNET.ENCRYPTION_SERVER
  REQUIRED
OPTIONSETTINGS  SHA1,MD5  STATIC  STRING  SHA1,MD5  Specifies list of
  checksumming algorithms in order of intended use  True  True
  SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER  SHA1,MD5
OPTIONSETTINGS  ACCEPTED,REJECTED,REQUESTED,REQUIRED  STATIC  STRING
  REQUESTED  Specifies the desired data integrity behavior  False  True
  SQLNET.CRYPTO_CHECKSUM_SERVER  REQUESTED
```

RDS API

To modify an option setting, use the Amazon RDS API [ModifyOptionGroup](#) command with the option group and option that you want to modify. By default, the option is enabled for each associated DB instance during its next maintenance window. To apply the change immediately to all associated DB instances, include the `ApplyImmediately` parameter and set it to `true`.

Removing an option from an option group

Some options can be removed from an option group, and some cannot. A persistent option cannot be removed from an option group until all DB instances associated with that option group are disassociated. A permanent option can never be removed from an option group. For more information about what options are removable, see the documentation for your specific engine listed at [Working with option groups \(p. 273\)](#).

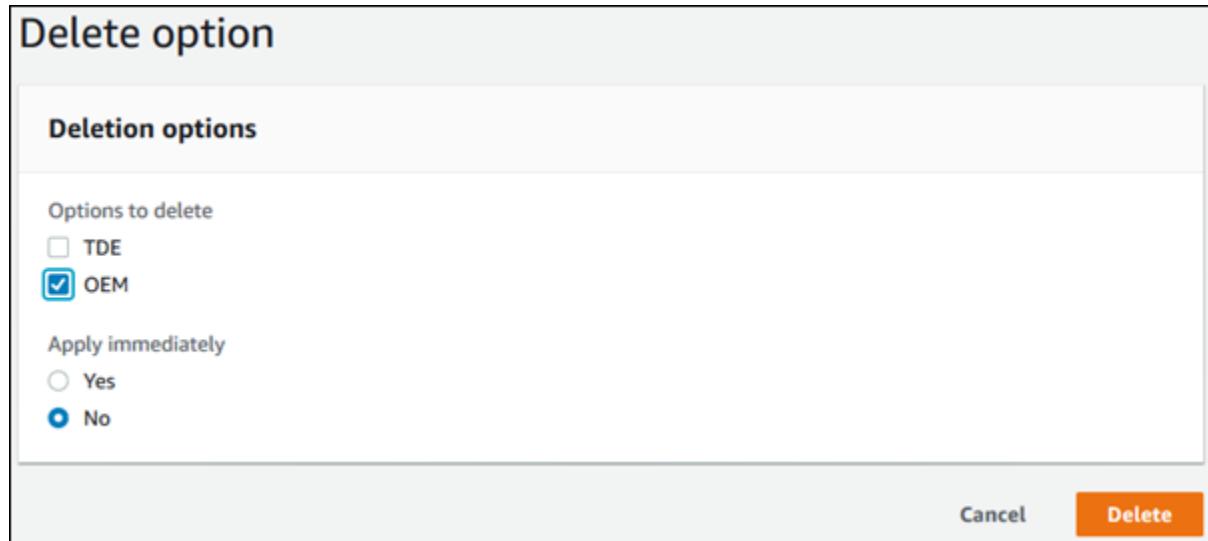
If you remove all options from an option group, Amazon RDS doesn't delete the option group. DB instances that are associated with the empty option group continue to be associated with it; they just won't have any active options. Alternatively, to remove all options from a DB instance, you can associate the DB instance with the default (empty) option group.

Console

You can use the AWS Management Console to remove an option from an option group.

To remove an option from an option group by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Select the option group whose option you want to remove, and then choose **Delete option**.
4. In the **Delete option** window, do the following:
 - Select the check box for the option that you want to delete.
 - For the deletion to take effect as soon as you make it, for **Apply immediately**, choose **Yes**. If you choose **No** (the default), the option is deleted for each associated DB instance during its next maintenance window.



5. When the settings are as you want them, choose **Yes, Delete**.

AWS CLI

To remove an option from an option group, use the AWS CLI `remove-option-from-option-group` command with the option that you want to delete. By default, the option is removed from each associated DB instance during its next maintenance window. To apply the change immediately, include the `--apply-immediately` parameter.

Example

The following example removes the Oracle Enterprise Manager Database Control (OEM) option from an option group named `testoptiongroup` and immediately applies the change.

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
  --option-group-name testoptiongroup \
  --options OEM \
  --apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
  --option-group-name testoptiongroup ^
  --options OEM ^
  --apply-immediately
```

Command output is similar to the following:

OPTIONGROUP	testoptiongroup	oracle-ee	12.1	Test option group
-------------	-----------------	-----------	------	-------------------

RDS API

To remove an option from an option group, use the Amazon RDS API `ModifyOptionGroup` action. By default, the option is removed from each associated DB instance during its next maintenance window. To apply the change immediately, include the `ApplyImmediately` parameter and set it to `true`.

Include the following parameters:

- `OptionGroupName`
- `OptionsToRemove.OptionName`

Deleting an option group

You can delete an option group that is not associated with any Amazon RDS resource. An option group can be associated with a DB instance, a manual DB snapshot, or an automated DB snapshot.

You can't delete a default option group. If you try to delete an option group that is associated with an RDS resource, an error like the following is returned.

An error occurred (InvalidOptionGroupStateFault) when calling the DeleteOptionGroup operation: The option group 'optionGroupName' cannot be deleted because it is in use.

To find the Amazon RDS resources associated with an option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the name of the option group to show its details.
4. Check the **Associated Instances and Snapshots** section for the associated Amazon RDS resources.

If a DB instance is associated with the option group, modify the DB instance to use a different option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If a manual DB snapshot is associated with the option group, modify the DB snapshot to use a different option group. You can do so using the AWS CLI `modify-db-snapshot` command.

Note

You can't modify the option group of an automated DB snapshot.

Console

One way of deleting an option group is by using the AWS Management Console.

To delete an option group by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group.
4. Choose **Delete group**.
5. On the confirmation page, choose **Delete** to finish deleting the option group, or choose **Cancel** to cancel the deletion.

AWS CLI

To delete an option group, use the AWS CLI `delete-option-group` command with the following required parameter.

- `--option-group-name`

Example

The following example deletes an option group named `testoptiongroup`.

For Linux, macOS, or Unix:

```
aws rds delete-option-group \
--option-group-name testoptiongroup
```

For Windows:

```
aws rds delete-option-group ^
--option-group-name testoptiongroup
```

RDS API

To delete an option group, call the Amazon RDS API [DeleteOptionGroup](#) operation. Include the following parameter:

- OptionGroupName

Working with parameter groups

Database parameters specify how the database is configured. For example, database parameters can specify the amount of resources, such as memory, to allocate to a database.

You manage your database configuration by associating your DB instances and Multi-AZ DB clusters with parameter groups. Amazon RDS defines parameter groups with default settings.

Important

You can define your own parameter groups with customized settings. Then you can modify your DB instances and Multi-AZ DB clusters to use your own parameter groups.

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#). For information about modifying a Multi-AZ DB clusters, see [Modifying a Multi-AZ DB cluster \(p. 341\)](#).

Note

Some DB engines offer additional features that you can add to your database as options in an option group. For information about option groups, see [Working with option groups \(p. 273\)](#).

A *DB parameter group* acts as a container for engine configuration values that are applied to one or more DB instances.

DB cluster parameter groups only apply to Multi-AZ DB clusters. In a Multi-AZ DB cluster, the settings in the DB cluster parameter group are used for all of the DB instances in the cluster. The default DB parameter group for the DB engine and DB engine version is used for each DB instance in the DB cluster.

If you create a DB instance without specifying a DB parameter group, the DB instance uses a default DB parameter group. Likewise, if you create a Multi-AZ DB cluster without specifying a DB cluster parameter group, the DB cluster uses a default DB cluster parameter group. Each default parameter group contains database engine defaults and Amazon RDS system defaults based on the engine, compute class, and allocated storage of the instance. You can't modify the parameter settings of a default parameter group. Instead, you create your own parameter group where you choose your own parameter settings. Not all DB engine parameters can be changed in a parameter group that you create.

To use your own parameter group, you create a new parameter group and modify the parameters that you want to modify. You then modify your DB instance or DB cluster to use the new parameter group. If you update parameters within a DB parameter group, the changes apply to all DB instances that are associated with that parameter group. Likewise, if you update parameters within a Multi-AZ DB cluster parameter group, the changes apply to all Aurora clusters that are associated with that DB cluster parameter group.

You can copy an existing DB parameter group with the AWS CLI [copy-db-parameter-group](#) command. You can copy an existing DB cluster parameter group with the AWS CLI [copy-db-cluster-parameter-group](#) command. Copying a parameter group can be convenient in some cases. An example is when you want to include most of an existing DB parameter group's custom parameters and values in a new DB parameter group.

Here are some important points about working with parameters in a parameter group:

- DB instance parameters are either *static* or *dynamic*. When you change a static parameter and save the DB parameter group, the parameter change takes effect after you manually reboot the associated DB instances.

When you change a dynamic parameter, by default the parameter change is applied to your DB instance immediately, without requiring a reboot. To defer the parameter change until after an associated DB instance is rebooted, use the AWS CLI or RDS API. Set the `ApplyMethod` to `pending-reboot` for the parameter change.

When you use the AWS Management Console to change DB instance parameter values, it always uses `immediate` for the `ApplyMethod` for dynamic parameters. For static parameters, the AWS Management Console always uses `pending-reboot` for the `ApplyMethod`.

For more information about using the AWS CLI to change a parameter value, see [modify-db-parameter-group](#). For more information about using the RDS API to change a parameter value, see [ModifyDBParameterGroup](#).

Note

Using `pending-reboot` with dynamic parameters in the AWS CLI or RDS API on RDS for SQL Server DB instances generates an error. Use `apply-immediately` on RDS for SQL Server.

- DB cluster parameters are either *static* or *dynamic*. When you change a static parameter and save the DB cluster parameter group, the parameter change takes effect after you manually reboot the associated DB clusters.

When you change a dynamic parameter, by default the parameter change is applied to your DB cluster immediately, without requiring a reboot. To defer the parameter change until after an associated DB cluster is rebooted, use the AWS CLI or RDS API. Set the `ApplyMethod` to `pending-reboot` for the parameter change.

When you use the AWS Management Console to change DB cluster parameter values, it always uses `immediate` for the `ApplyMethod` for dynamic parameters. For static parameters, the console always uses `pending-reboot` for the `ApplyMethod`.

For more information about using the AWS CLI to change a parameter value, see [modify-db-cluster-parameter-group](#). For more information about using the RDS API to change a parameter value, see [ModifyDBClusterParameterGroup](#).

- If a DB instance isn't using the latest changes to its associated DB parameter group, the console shows a status of `pending-reboot` for the DB parameter group. This status doesn't result in an automatic reboot during the next maintenance window. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.
- When you associate a new DB parameter group with a DB instance, the modified static and dynamic parameters are applied only after the DB instance is rebooted. However, if you modify dynamic parameters in the newly associated DB parameter group, these changes are applied immediately without a reboot. For more information about changing the DB parameter group, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- After you change the DB cluster parameter group associated with a Multi-AZ DB cluster, reboot the DB cluster. Doing this applies the changes to all of the DB instances in the DB cluster.

For information about rebooting a Multi-AZ DB cluster, see [Rebooting Multi-AZ DB clusters and reader DB instances \(p. 368\)](#).

- In many cases, you can specify integer and Boolean parameter values using expressions, formulas, and functions. Functions can include a mathematical log expression. However, not all parameters support expressions, formulas, and functions for parameter values. For more information, see [Specifying DB parameters \(p. 310\)](#).
- Set any parameters that relate to the character set or collation of your database in your parameter group before creating the DB instance or Multi-AZ DB cluster. Also do so before you create a database in it. This ensures that the default database and new databases use the character set and collation values that you specify. If you change character set or collation parameters, the parameter changes aren't applied to existing databases.

For some DB engines, you can change character set or collation values for an existing database using the `ALTER DATABASE` command, for example:

```
ALTER DATABASE database_name CHARACTER SET character_set_name COLLATE collation;
```

For more information about changing the character set or collation values for a database, check the documentation for your DB engine.

- Improperly setting parameters in a parameter group can have unintended adverse effects, including degraded performance and system instability. Always be cautious when modifying database parameters, and back up your data before modifying a parameter group. Try parameter group setting changes on a test DB instance or DB cluster before applying those parameter group changes to a production DB instance or DB cluster.
- To determine the supported parameters for your DB engine, view the parameters in the DB parameter group and DB cluster parameter group used by the DB instance or DB cluster. For more information, see [Viewing parameter values for a DB parameter group \(p. 301\)](#) and [Viewing parameter values for a DB cluster parameter group \(p. 309\)](#).

Topics

- [Working with DB parameter groups \(p. 291\)](#)
- [Working with DB cluster parameter groups for Multi-AZ DB clusters \(p. 302\)](#)
- [Comparing parameter groups \(p. 310\)](#)
- [Specifying DB parameters \(p. 310\)](#)

Working with DB parameter groups

DB instances use DB parameter groups. The following sections describe configuring and managing DB instance parameter groups.

Topics

- [Creating a DB parameter group \(p. 291\)](#)
- [Associating a DB parameter group with a DB instance \(p. 293\)](#)
- [Modifying parameters in a DB parameter group \(p. 294\)](#)
- [Resetting parameters in a DB parameter group to their default values \(p. 296\)](#)
- [Copying a DB parameter group \(p. 298\)](#)
- [Listing DB parameter groups \(p. 300\)](#)
- [Viewing parameter values for a DB parameter group \(p. 301\)](#)

Creating a DB parameter group

You can create a new DB parameter group using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To create a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.

The **Create parameter group** window appears.

4. In the **Parameter group family** list, select a DB parameter group family.

5. In the **Type** list, select **DB Parameter Group**.
6. In the **Group name** box, enter the name of the new DB parameter group.
7. In the **Description** box, enter a description for the new DB parameter group.
8. Choose **Create**.

AWS CLI

To create a DB parameter group, use the AWS CLI `create-db-parameter-group` command. The following example creates a DB parameter group named *mydbparametergroup* for MySQL version 8.0 with a description of "My new parameter group."

Include the following required parameters:

- `--db-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

To list all of the available parameter group families, use the following command:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

Note

The output contains duplicates.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
  --db-parameter-group-name mydbparametergroup \
  --db-parameter-group-family MySQL8.0 \
  --description "My new parameter group"
```

For Windows:

```
aws rds create-db-parameter-group ^
  --db-parameter-group-name mydbparametergroup ^
  --db-parameter-group-family MySQL8.0 ^
  --description "My new parameter group"
```

This command produces output similar to the following:

```
DBPARAMETERGROUP  mydbparametergroup  mysql8.0  My new parameter group
```

RDS API

To create a DB parameter group, use the RDS API `CreateDBParameterGroup` operation.

Include the following required parameters:

- `DBParameterGroupName`
- `DBParameterGroupFamily`

- Description

Associating a DB parameter group with a DB instance

You can create your own DB parameter groups with customized settings. You can associate a DB parameter group with a DB instance using the AWS Management Console, the AWS CLI, or the RDS API. You can do so when you create or modify a DB instance.

For information about creating a DB parameter group, see [Creating a DB parameter group \(p. 291\)](#). For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#). For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

When you associate a new DB parameter group with a DB instance, the modified static and dynamic parameters are applied only after the DB instance is rebooted. However, if you modify dynamic parameters in the newly associated DB parameter group, these changes are applied immediately without a reboot.

Console

To associate a DB parameter group with a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB Instance** page appears.
4. Change the **DB parameter group** setting.
5. Choose **Continue** and check the summary of modifications.
6. (Optional) Choose **Apply immediately** to apply the changes immediately. Choosing this option can cause an outage in some cases. For more information, see [Using the Apply Immediately setting \(p. 328\)](#).
7. On the confirmation page, review your changes. If they are correct, choose **Modify DB instance** to save your changes.

Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

AWS CLI

To associate a DB parameter group with a DB instance, use the AWS CLI `modify-db-instance` command with the following options:

- `--db-instance-identifier`
- `--db-parameter-group-name`

The following example associates the `mydbpg` DB parameter group with the `database-1` DB instance. The changes are applied immediately by using `--apply-immediately`. Use `--no-apply-immediately` to apply the changes during the next maintenance window. For more information, see [Using the Apply Immediately setting \(p. 328\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier database-1 \
--db-parameter-group-name mydbpg \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier database-1 ^
--db-parameter-group-name mydbpg ^
--apply-immediately
```

RDS API

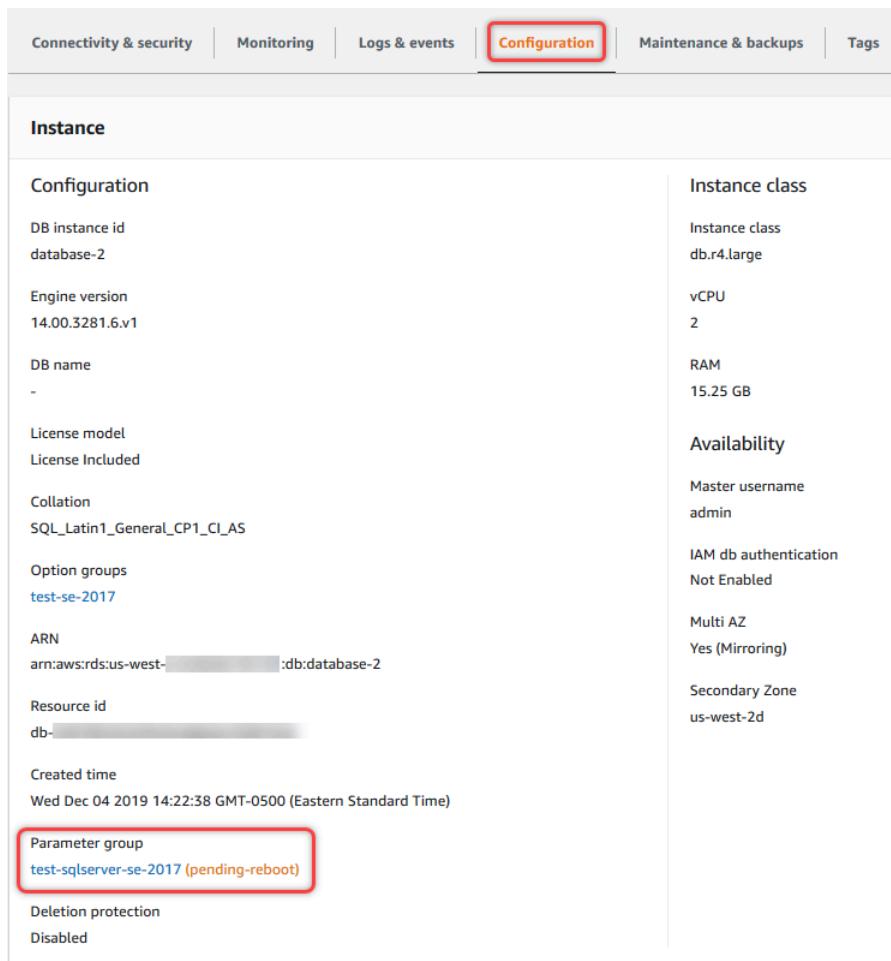
To associate a DB parameter group with a DB instance, use the RDS API [ModifyDBInstance](#) operation with the following parameters:

- `DBInstanceName`
- `DBParameterGroupName`

Modifying parameters in a DB parameter group

You can modify parameter values in a customer-created DB parameter group; you can't change the parameter values in a default DB parameter group. Changes to parameters in a customer-created DB parameter group are applied to all DB instances that are associated with the DB parameter group.

Changes to some parameters are applied to the DB instance immediately without a reboot. Changes to other parameters are applied only after the DB instance is rebooted. The RDS console shows the status of the DB parameter group associated with a DB instance on the **Configuration** tab. For example, suppose that the DB instance isn't using the latest changes to its associated DB parameter group. If so, the RDS console shows the DB parameter group with a status of **pending-reboot**. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.



The screenshot shows the AWS Management Console interface for an Amazon RDS instance. The top navigation bar has tabs: Connectivity & security, Monitoring, Logs & events, Configuration (which is highlighted with a red box), Maintenance & backups, and Tags. Below the tabs, the page title is "Instance". The left sidebar lists "Configuration" sections: DB instance id (database-2), Engine version (14.00.3281.6.v1), DB name (-), License model (License Included), Collation (SQL_Latin1_General_CI_AS), Option groups (test-se-2017), ARN (arn:aws:rds:us-west-2:XXXXXXXXXX:db:database-2), Resource id (db-XXXXXX), and Created time (Wed Dec 04 2019 14:22:38 GMT-0500 (Eastern Standard Time)). A red box highlights the "Parameter group" section, which contains "test-sqlserver-se-2017 (pending-reboot)". The right sidebar lists "Instance class" (db.r4.large), vCPU (2), RAM (15.25 GB), and "Availability" (Master username: admin, IAM db authentication: Not Enabled, Multi AZ: Yes (Mirroring), Secondary Zone: us-west-2d).

Console

To modify a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group that you want to modify.
4. For **Parameter group actions**, choose **Edit**.
5. Change the values of the parameters that you want to modify. You can scroll through the parameters using the arrow keys at the top right of the dialog box.

You can't change values in a default parameter group.
6. Choose **Save changes**.

AWS CLI

To modify a DB parameter group, use the AWS CLI `modify-db-parameter-group` command with the following required options:

- `--db-parameter-group-name`

- **--parameters**

The following example modifies the `max_connections` and `max_allowed_packet` values in the DB parameter group named `mydbparametergroup`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name mydbparametergroup \
  --parameters "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" \
  "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name mydbparametergroup ^
  --parameters "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" ^
  "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

The command produces output like the following:

```
DBPARAMETERGROUP mydbparametergroup
```

RDS API

To modify a DB parameter group, use the RDS API [ModifyDBParameterGroup](#) operation with the following required parameters:

- `DBParameterGroupName`
- `Parameters`

Resetting parameters in a DB parameter group to their default values

You can reset parameter values in a customer-created DB parameter group to their default values. Changes to parameters in a customer-created DB parameter group are applied to all DB instances that are associated with the DB parameter group.

When you use the console, you can reset specific parameters to their default values. However, you can't easily reset all of the parameters in the DB parameter group at once. When you use the AWS CLI or RDS API, you can reset specific parameters to their default values. You can also reset all of the parameters in the DB parameter group at once.

Changes to some parameters are applied to the DB instance immediately without a reboot. Changes to other parameters are applied only after the DB instance is rebooted. The RDS console shows the status of the DB parameter group associated with a DB instance on the **Configuration** tab. For example, suppose that the DB instance isn't using the latest changes to its associated DB parameter group. If so, the RDS console shows the DB parameter group with a status of **pending-reboot**. To apply the latest parameter changes to that DB instance, manually reboot the DB instance.

Configuration	Instance class
DB instance id database-2	Instance class db.r4.large
Engine version 14.00.3281.6.v1	vCPU 2
DB name -	RAM 15.25 GB
License model License Included	Availability
Collation SQL_Latin1_General_CI_AS	Master username admin
Option groups test-se-2017	IAM db authentication Not Enabled
ARN arn:aws:rds:us-west-2:123456789012:db:database-2	Multi AZ Yes (Mirroring)
Resource id db-12345678	Secondary Zone us-west-2d
Created time Wed Dec 04 2019 14:22:38 GMT-0500 (Eastern Standard Time)	
Parameter group test-sqlserver-se-2017 (pending-reboot)	
Deletion protection Disabled	

Note

In a default DB parameter group, parameters are always set to their default values.

Console

To reset parameters in a DB parameter group to their default values

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group.
4. For **Parameter group actions**, choose **Edit**.
5. Choose the parameters that you want to reset to their default values. You can scroll through the parameters using the arrow keys at the top right of the dialog box.

You can't reset values in a default parameter group.

6. Choose **Reset** and then confirm by choosing **Reset parameters**.

AWS CLI

To reset some or all of the parameters in a DB parameter group, use the AWS CLI `reset-db-parameter-group` command with the following required option: `--db-parameter-group-name`.

To reset all of the parameters in the DB parameter group, specify the `--reset-all-parameters` option. To reset specific parameters, specify the `--parameters` option.

The following example resets all of the parameters in the DB parameter group named *mydbparametergroup* to their default values.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-parameter-group \
--db-parameter-group-name mydbparametergroup \
--reset-all-parameters
```

For Windows:

```
aws rds reset-db-parameter-group ^
--db-parameter-group-name mydbparametergroup ^
--reset-all-parameters
```

The following example resets the `max_connections` and `max_allowed_packet` options to their default values in the DB parameter group named *mydbparametergroup*.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-parameter-group \
--db-parameter-group-name mydbparametergroup \
--parameters "ParameterName=max_connections,ApplyMethod=immediate" \
"ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

For Windows:

```
aws rds reset-db-parameter-group ^
--db-parameter-group-name mydbparametergroup ^
--parameters "ParameterName=max_connections,ApplyMethod=immediate" ^
"ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

The command produces output like the following:

```
DBParameterGroupName mydbparametergroup
```

RDS API

To reset parameters in a DB parameter group to their default values, use the RDS API [ResetDBParameterGroup](#) command with the following required parameter: `DBParameterGroupName`.

To reset all of the parameters in the DB parameter group, set the `ResetAllParameters` parameter to `true`. To reset specific parameters, specify the `Parameters` parameter.

Copying a DB parameter group

You can copy custom DB parameter groups that you create. Copying a parameter group can be convenient solution. An example is when you have created a DB parameter group and want to include

most of its custom parameters and values in a new DB parameter group. You can copy a DB parameter group by using the AWS Management Console. You can also use the AWS CLI [copy-db-parameter-group](#) command or the RDS API [CopyDBParameterGroup](#) operation.

After you copy a DB parameter group, wait at least 5 minutes before creating your first DB instance that uses that DB parameter group as the default parameter group. Doing this allows Amazon RDS to fully complete the copy action before the parameter group is used. This is especially important for parameters that are critical when creating the default database for a DB instance. An example is the character set for the default database defined by the `character_set_database` parameter. Use the **Parameter Groups** option of the [Amazon RDS console](#) or the [describe-db-parameters](#) command to verify that your DB parameter group is created.

Note

You can't copy a default parameter group. However, you can create a new parameter group that is based on a default parameter group.

Currently, you can't copy a parameter group to a different AWS Region.

Console

To copy a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the custom parameter group that you want to copy.
4. For **Parameter group actions**, choose **Copy**.
5. In **New DB parameter group identifier**, enter a name for the new parameter group.
6. In **Description**, enter a description for the new parameter group.
7. Choose **Copy**.

AWS CLI

To copy a DB parameter group, use the AWS CLI [copy-db-parameter-group](#) command with the following required options:

- `--source-db-parameter-group-identifier`
- `--target-db-parameter-group-identifier`
- `--target-db-parameter-group-description`

The following example creates a new DB parameter group named `mygroup2` that is a copy of the DB parameter group `mygroup1`.

Example

For Linux, macOS, or Unix:

```
aws rds copy-db-parameter-group \
  --source-db-parameter-group-identifier mygroup1 \
  --target-db-parameter-group-identifier mygroup2 \
  --target-db-parameter-group-description "DB parameter group 2"
```

For Windows:

```
aws rds copy-db-parameter-group ^
```

```
--source-db-parameter-group-identifier mygroup1 ^
--target-db-parameter-group-identifier mygroup2 ^
--target-db-parameter-group-description "DB parameter group 2"
```

RDS API

To copy a DB parameter group, use the RDS API [CopyDBParameterGroup](#) operation with the following required parameters:

- `SourceDBParameterGroupIdentifier`
- `TargetDBParameterGroupIdentifier`
- `TargetDBParameterGroupDescription`

Listing DB parameter groups

You can list the DB parameter groups you've created for your AWS account.

Note

Default parameter groups are automatically created from a default parameter template when you create a DB instance for a particular DB engine and version. These default parameter groups contain preferred parameter settings and can't be modified. When you create a custom parameter group, you can modify parameter settings.

Console

To list all DB parameter groups for an AWS account

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.

The DB parameter groups appear in a list.

AWS CLI

To list all DB parameter groups for an AWS account, use the AWS CLI [describe-db-parameter-groups](#) command.

Example

The following example lists all available DB parameter groups for an AWS account.

```
aws rds describe-db-parameter-groups
```

The command returns a response like the following:

```
DBPARAMETERGROUP default.mysql8.0      mysql8.0  Default parameter group for MySQL8.0
DBPARAMETERGROUP mydbparametergroup     mysql8.0  My new parameter group
```

The following example describes the *mydbparamgroup1* parameter group.

For Linux, macOS, or Unix:

```
aws rds describe-db-parameter-groups \
```

```
--db-parameter-group-name mydbparamgroup1
```

For Windows:

```
aws rds describe-db-parameter-groups ^
--db-parameter-group-name mydbparamgroup1
```

The command returns a response like the following:

```
DBPARAMETERGROUP mydbparametergroup1 mysql8.0 My new parameter group
```

RDS API

To list all DB parameter groups for an AWS account, use the RDS API [DescribeDBParameterGroups](#) operation.

Viewing parameter values for a DB parameter group

You can get a list of all parameters in a DB parameter group and their values.

Console

To view the parameter values for a DB parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
The DB parameter groups appear in a list.
3. Choose the name of the parameter group to see its list of parameters.

AWS CLI

To view the parameter values for a DB parameter group, use the AWS CLI [describe-db-parameters](#) command with the following required parameter.

- `--db-parameter-group-name`

Example

The following example lists the parameters and parameter values for a DB parameter group named *mydbparametergroup*.

```
aws rds describe-db-parameters --db-parameter-group-name mydbparametergroup
```

The command returns a response like the following:

DBPARAMETER Type	Parameter Name	Parameter Value	Source	Data Type	Apply
DBPARAMETER Is Modifiable					
DBPARAMETER	allow-suspicious-udfs		engine-default	boolean	static
	false				
DBPARAMETER	auto_increment_increment		engine-default	integer	dynamic
	true				
DBPARAMETER	auto_increment_offset		engine-default	integer	dynamic
	true				

DBPARAMETER	binlog_cache_size	32768	system	integer	dynamic
DBPARAMETER	socket	/tmp/mysql.sock	system	string	static

RDS API

To view the parameter values for a DB parameter group, use the RDS API [DescribeDBParameters](#) command with the following required parameter.

- `DBParameterGroupName`

Working with DB cluster parameter groups for Multi-AZ DB clusters

Multi-AZ DB clusters use DB cluster parameter groups. The following sections describe configuring and managing DB cluster parameter groups.

Topics

- [Creating a DB cluster parameter group \(p. 302\)](#)
- [Modifying parameters in a DB cluster parameter group \(p. 304\)](#)
- [Resetting parameters in a DB cluster parameter group \(p. 305\)](#)
- [Copying a DB cluster parameter group \(p. 306\)](#)
- [Listing DB cluster parameter groups \(p. 308\)](#)
- [Viewing parameter values for a DB cluster parameter group \(p. 309\)](#)

Creating a DB cluster parameter group

You can create a new DB cluster parameter group using the AWS Management Console, the AWS CLI, or the RDS API.

After you create a DB cluster parameter group, wait at least 5 minutes before creating a DB cluster that uses that DB cluster parameter group. Doing this allows Amazon RDS to fully create the parameter group before it is used by the new DB cluster. You can use the **Parameter groups** page in the [Amazon RDS console](#) or the `describe-db-cluster-parameters` command to verify that your DB cluster parameter group is created.

Console

To create a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.

The **Create parameter group** window appears.

4. In the **Parameter group family** list, select a DB parameter group family
5. In the **Type** list, select **DB Cluster Parameter Group**.
6. In the **Group name** box, enter the name of the new DB cluster parameter group.
7. In the **Description** box, enter a description for the new DB cluster parameter group.

8. Choose **Create**.

AWS CLI

To create a DB cluster parameter group, use the AWS CLI [create-db-cluster-parameter-group](#) command.

The following example creates a DB cluster parameter group named *mydbclusterparametergroup* for RDS for MySQL version 8.0 with a description of "My new cluster parameter group."

Include the following required parameters:

- `--db-cluster-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

To list all of the available parameter group families, use the following command:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

Note

The output contains duplicates.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --db-parameter-group-family mysql8.0 \
    --description "My new cluster parameter group"
```

For Windows:

```
aws rds create-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --db-parameter-group-family mysql8.0 ^
    --description "My new cluster parameter group"
```

This command produces output similar to the following:

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "mydbclusterparametergroup",
        "DBParameterGroupFamily": "mysql8.0",
        "Description": "My new cluster parameter group",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup2"
    }
}
```

RDS API

To create a DB cluster parameter group, use the RDS API [CreateDBClusterParameterGroup](#) action.

Include the following required parameters:

- `DBClusterParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Modifying parameters in a DB cluster parameter group

You can modify parameter values in a customer-created DB cluster parameter group. You can't change the parameter values in a default DB cluster parameter group. Changes to parameters in a customer-created DB cluster parameter group are applied to all DB clusters that are associated with the DB cluster parameter group.

Console

To modify a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group that you want to modify.
4. For **Parameter group actions**, choose **Edit**.
5. Change the values of the parameters you want to modify. You can scroll through the parameters using the arrow keys at the top right of the dialog box.

You can't change values in a default parameter group.
6. Choose **Save changes**.
7. Reboot the primary DB instance in the cluster to apply the changes to all of the DB instances in the cluster.

AWS CLI

To modify a DB cluster parameter group, use the AWS CLI `modify-db-cluster-parameter-group` command with the following required parameters:

- `--db-cluster-parameter-group-name`
- `--parameters`

The following example modifies the `server_audit_logging` and `server_audit_logs_upload` values in the DB cluster parameter group named `mydbclusterparametergroup`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name mydbclusterparametergroup \
  --parameters
  "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" \
  "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-cluster-parameter-group ^
```

```
--db-cluster-parameter-group-name mydbclusterparametergroup ^
--parameters
"ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^
"ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

The command produces output like the following:

```
DBCLUSTERPARAMETERGROUP mydbclusterparametergroup
```

RDS API

To modify a DB cluster parameter group, use the RDS API [ModifyDBClusterParameterGroup](#) command with the following required parameters:

- `DBClusterParameterGroupName`
- `Parameters`

Resetting parameters in a DB cluster parameter group

You can reset parameters to their default values in a customer-created DB cluster parameter group. Changes to parameters in a customer-created DB cluster parameter group are applied to all DB clusters that are associated with the DB cluster parameter group.

Note

In a default DB cluster parameter group, parameters are always set to their default values.

Console

To reset parameters in a DB cluster parameter group to their default values

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the parameter group.
4. For **Parameter group actions**, choose **Edit**.
5. Choose the parameters that you want to reset to their default values. You can scroll through the parameters using the arrow keys at the top right of the dialog box.

You can't reset values in a default parameter group.
6. Choose **Reset** and then confirm by choosing **Reset parameters**.
7. Reboot the primary DB instance in the DB cluster to apply the changes to all of the DB instances in the DB cluster.

AWS CLI

To reset parameters in a DB cluster parameter group to their default values, use the AWS CLI [reset-db-cluster-parameter-group](#) command with the following required option: `--db-cluster-parameter-group-name`.

To reset all of the parameters in the DB cluster parameter group, specify the `--reset-all-parameters` option. To reset specific parameters, specify the `--parameters` option.

The following example resets all of the parameters in the DB parameter group named `mydbparametergroup` to their default values.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-cluster-parameter-group \
--db-cluster-parameter-group-name mydbparametergroup \
--reset-all-parameters
```

For Windows:

```
aws rds reset-db-cluster-parameter-group ^
--db-cluster-parameter-group-name mydbparametergroup ^
--reset-all-parameters
```

The following example resets the `server_audit_logging` and `server_audit_logs_upload` to their default values in the DB cluster parameter group named `mydbclusterparametergroup`.

Example

For Linux, macOS, or Unix:

```
aws rds reset-db-cluster-parameter-group \
--db-cluster-parameter-group-name mydbclusterparametergroup \
--parameters "ParameterName=server_audit_logging,ApplyMethod=immediate" \
"ParameterName=server_audit_logs_upload,ApplyMethod=immediate"
```

For Windows:

```
aws rds reset-db-cluster-parameter-group ^
--db-cluster-parameter-group-name mydbclusterparametergroup ^
--parameters
"ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^
"ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

The command produces output like the following:

```
DBClusterParameterGroupName mydbclusterparametergroup
```

RDS API

To reset parameters in a DB cluster parameter group to their default values, use the RDS API [ResetDBClusterParameterGroup](#) command with the following required parameter: `DBClusterParameterGroupName`.

To reset all of the parameters in the DB cluster parameter group, set the `ResetAllParameters` parameter to `true`. To reset specific parameters, specify the `Parameters` parameter.

Copying a DB cluster parameter group

You can copy custom DB cluster parameter groups that you create. Copying a parameter group is a convenient solution when you have already created a DB cluster parameter group and you want to include most of the custom parameters and values from that group in a new DB cluster parameter group. You can copy a DB cluster parameter group by using the AWS CLI [copy-db-cluster-parameter-group](#) command or the RDS API [CopyDBClusterParameterGroup](#) operation.

After you copy a DB cluster parameter group, wait at least 5 minutes before creating a DB cluster that uses that DB cluster parameter group. Doing this allows Amazon RDS to fully copy the parameter group before it is used by the new DB cluster. You can use the **Parameter groups** page in the [Amazon RDS console](#) or the `describe-db-cluster-parameters` command to verify that your DB cluster parameter group is created.

Note

You can't copy a default parameter group. However, you can create a new parameter group that is based on a default parameter group.

Console

To copy a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the custom parameter group that you want to copy.
4. For **Parameter group actions**, choose **Copy**.
5. In **New DB parameter group identifier**, enter a name for the new parameter group.
6. In **Description**, enter a description for the new parameter group.
7. Choose **Copy**.

AWS CLI

To copy a DB cluster parameter group, use the AWS CLI `copy-db-cluster-parameter-group` command with the following required parameters:

- `--source-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-description`

The following example creates a new DB cluster parameter group named `mygroup2` that is a copy of the DB cluster parameter group `mygroup1`.

Example

For Linux, macOS, or Unix:

```
aws rds copy-db-cluster-parameter-group \
  --source-db-cluster-parameter-group-identifier mygroup1 \
  --target-db-cluster-parameter-group-identifier mygroup2 \
  --target-db-cluster-parameter-group-description "DB parameter group 2"
```

For Windows:

```
aws rds copy-db-cluster-parameter-group ^
  --source-db-cluster-parameter-group-identifier mygroup1 ^
  --target-db-cluster-parameter-group-identifier mygroup2 ^
  --target-db-cluster-parameter-group-description "DB parameter group 2"
```

RDS API

To copy a DB cluster parameter group, use the RDS API `CopyDBClusterParameterGroup` operation with the following required parameters:

- `SourceDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupDescription`

List DB cluster parameter groups

You can list the DB cluster parameter groups you've created for your AWS account.

Note

Default parameter groups are automatically created from a default parameter template when you create a DB cluster for a particular DB engine and version. These default parameter groups contain preferred parameter settings and can't be modified. When you create a custom parameter group, you can modify parameter settings.

Console

To list all DB cluster parameter groups for an AWS account

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.

The DB cluster parameter groups appear in the list with **DB cluster parameter group** for Type.

AWS CLI

To list all DB cluster parameter groups for an AWS account, use the AWS CLI [describe-db-cluster-parameter-groups](#) command.

Example

The following example lists all available DB cluster parameter groups for an AWS account.

```
aws rds describe-db-cluster-parameter-groups
```

The following example describes the *mydbclusterparametergroup* parameter group.

For Linux, macOS, or Unix:

```
aws rds describe-db-cluster-parameter-groups \
--db-cluster-parameter-group-name mydbclusterparametergroup
```

For Windows:

```
aws rds describe-db-cluster-parameter-groups ^
--db-cluster-parameter-group-name mydbclusterparametergroup
```

The command returns a response like the following:

```
{
  "DBClusterParameterGroups": [
    {
      "DBClusterParameterGroupName": "mydbclusterparametergroup2",
      "DBParameterGroupFamily": "mysql8.0",
```

```
        "Description": "My new cluster parameter group",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup"
    }
]
```

RDS API

To list all DB cluster parameter groups for an AWS account, use the RDS API [DescribeDBClusterParameterGroups](#) action.

Viewing parameter values for a DB cluster parameter group

You can get a list of all parameters in a DB cluster parameter group and their values.

Console

To view the parameter values for a DB cluster parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
The DB cluster parameter groups appear in the list with **DB cluster parameter group** for Type.
3. Choose the name of the DB cluster parameter group to see its list of parameters.

AWS CLI

To view the parameter values for a DB cluster parameter group, use the AWS CLI [describe-db-cluster-parameters](#) command with the following required parameter.

- `--db-cluster-parameter-group-name`

Example

The following example lists the parameters and parameter values for a DB cluster parameter group named *mydbclusterparametergroup*, in JSON format.

The command returns a response like the following:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-
name mydbclusterparametergroup
```

```
{
    "Parameters": [
        {
            "ParameterName": "activate_all_roles_on_login",
            "ParameterValue": "0",
            "Description": "Automatically set all granted roles as active after the user has authenticated successfully.",
            "Source": "engine-default",
            "ApplyType": "dynamic",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
```

```
        "SupportedEngineModes": [
            "provisioned"
        ]
    },
{
    "ParameterName": "allow-suspicious-udfs",
    "Description": "Controls whether user-defined functions that have only an xxx symbol for the main function can be loaded",
    "Source": "engine-default",
    "ApplyType": "static",
    "DataType": "boolean",
    "AllowedValues": "0,1",
    "IsModifiable": false,
    "ApplyMethod": "pending-reboot",
    "SupportedEngineModes": [
        "provisioned"
    ]
},
...
...
```

RDS API

To view the parameter values for a DB cluster parameter group, use the RDS API [DescribeDBClusterParameters](#) command with the following required parameter.

- `DBClusterParameterGroupName`

Comparing parameter groups

You can use the AWS Management Console to view the differences between two parameter groups.

To compare two parameter groups

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. In the list, choose the two parameter groups that you want to compare.
4. For **Parameter group actions**, choose **Compare**.

Note

The specified parameter groups must both be DB parameter groups, or they both must be DB cluster parameter groups. This is true even when the DB engine and version are the same. For example, you can't compare an Aurora MySQL 8.0 DB parameter group and an Aurora MySQL 8.0 DB cluster parameter group.

You can compare Aurora MySQL and RDS for MySQL DB parameter groups, even for different versions, but you can't compare Aurora PostgreSQL and RDS for PostgreSQL DB parameter groups.

Specifying DB parameters

DB parameter types include the following:

- Integer
- Boolean
- String
- Long

- Double
- Timestamp
- Object of other defined data types
- Array of values of type integer, Boolean, string, long, double, timestamp, or object

You can also specify integer and Boolean parameters using expressions, formulas, and functions.

For the Oracle engine, you can use the `DBInstanceClassHugePagesDefault` formula variable to specify a Boolean DB parameter. See [DB parameter formula variables \(p. 311\)](#).

For the PostgreSQL engine, you can use an expression to specify a Boolean DB parameter. See [Boolean DB parameter expressions \(p. 313\)](#).

Contents

- [DB parameter formulas \(p. 311\)](#)
 - [DB parameter formula variables \(p. 311\)](#)
 - [DB parameter formula operators \(p. 312\)](#)
- [DB parameter functions \(p. 312\)](#)
- [Boolean DB parameter expressions \(p. 313\)](#)
- [DB parameter log expressions \(p. 314\)](#)
- [DB parameter value examples \(p. 314\)](#)

DB parameter formulas

A DB parameter formula is an expression that resolves to an integer value or a Boolean value. You enclose the expression in braces: {} . You can use a formula for either a DB parameter value or as an argument to a DB parameter function.

Syntax

```
{FormulaVariable}
{FormulaVariable*Integer}
{FormulaVariable*Integer/Integer}
{FormulaVariable/Integer}
```

DB parameter formula variables

Each formula variable returns an integer or a Boolean value. The names of the variables are case-sensitive.

AllocatedStorage

Returns an integer representing the size, in bytes, of the data volume.

DBInstanceClassHugePagesDefault

Returns a Boolean value. Currently, it's only supported for Oracle engines.

For more information, see [Turning on HugePages for an RDS for Oracle instance \(p. 1610\)](#).

DBInstanceClassMemory

Returns an integer for the number of bytes of memory available to the database process. This number is internally calculated by starting with the total amount of memory for the DB instance class. From this, the calculation subtracts memory reserved for the operating system and the RDS

processes that manage the instance. Therefore, the number is always somewhat lower than the memory figures shown in the instance class tables in [DB instance classes \(p. 10\)](#). The exact value depends on a combination of factors. These include instance class, DB engine, and whether it applies to an RDS instance or an instance that's part of an Aurora cluster.

DBInstanceVCPU

Returns an integer representing the number of virtual central processing units (vCPUs) used by Amazon RDS to manage the instance. Currently, it's only supported for the PostgreSQL engine.

EndPointPort

Returns an integer representing the port used when connecting to the DB instance.

DB parameter formula operators

DB parameter formulas support two operators: division and multiplication.

Division operator: /

Divides the dividend by the divisor, returning an integer quotient. Decimals in the quotient are truncated, not rounded.

Syntax

```
dividend / divisor
```

The dividend and divisor arguments must be integer expressions.

*Multiplication operator: **

Multiplies the expressions, returning the product of the expressions. Decimals in the expressions are truncated, not rounded.

Syntax

```
expression * expression
```

Both expressions must be integers.

DB parameter functions

You specify the arguments of DB parameter functions as either integers or formulas. Each function must have at least one argument. Specify multiple arguments as a comma-separated list. The list can't have any empty members, such as *argument1,,argument3*. Function names are case-insensitive.

IF

Returns an argument.

Currently, it's only supported for Oracle engines, and the only supported first argument is {DBInstanceClassHugePagesDefault}. For more information, see [Turning on HugePages for an RDS for Oracle instance \(p. 1610\)](#).

Syntax

```
IF(argument1, argument2, argument3)
```

Returns the second argument if the first argument evaluates to true. Returns the third argument otherwise.

GREATEST

Returns the largest value from a list of integers or parameter formulas.

Syntax

```
GREATEST(argument1, argument2,...argumentn)
```

Returns an integer.

LEAST

Returns the smallest value from a list of integers or parameter formulas.

Syntax

```
LEAST(argument1, argument2,...argumentn)
```

Returns an integer.

SUM

Adds the values of the specified integers or parameter formulas.

Syntax

```
SUM(argument1, argument2,...argumentn)
```

Returns an integer.

Boolean DB parameter expressions

A Boolean DB parameter expression resolves to a Boolean value of 1 or 0. The expression is enclosed in quotation marks.

Note

Boolean DB parameter expressions are only supported for the PostgreSQL engine.

Syntax

```
"expression operator expression"
```

Both expressions must resolve to integers. An expression can be the following:

- integer constant
- DB parameter formula
- DB parameter function
- DB parameter variable

Boolean DB parameter expressions support the following inequality operators:

The greater than operator: >

Syntax

```
"expression > expression"
```

The less than operator: <

Syntax

```
"expression < expression"
```

The greater than or equal to operators: >=, =>

Syntax

```
"expression >= expression"  
"expression => expression"
```

The less than or equal to operators: <=, ==<

Syntax

```
"expression <= expression"  
"expression ==< expression"
```

Example using a Boolean DB parameter expression

The following Boolean DB parameter expression example compares the result of a parameter formula with an integer. It does so to modify the Boolean DB parameter wal_compression for a PostgreSQL DB instance. The parameter expression compares the number of vCPUs with the value 2. If the number of vCPUs is greater than 2, then the wal_compression DB parameter is set to true.

```
aws rds modify-db-parameter-group --db-parameter-group-name group-name \  
--parameters "ParameterName=wal_compression,ParameterValue=\\"{DBInstanceVCPU} > 2\\" "
```

DB parameter log expressions

You can set an integer DB parameter value to a log expression. You enclose the expression in braces: {}.

For example:

```
{log(DBInstanceClassMemory/8187281418)*1000}
```

The log function represents log base 2. This example also uses the DBInstanceClassMemory formula variable. See [DB parameter formula variables \(p. 311\)](#).

Note

Currently, you can't specify the MySQL innodb_log_file_size parameter with any value other than an integer.

DB parameter value examples

These examples show using formulas, functions, and expressions for the values of DB parameters.

Note

DB Parameter functions are currently supported only in the console and aren't supported in the AWS CLI.

Warning

Improperly setting parameters in a DB parameter group can have unintended adverse effects. These might include degraded performance and system instability. Use caution when modifying database parameters and back up your data before modifying your DB parameter group. Try out parameter group changes on a test DB instance, created using point-in-time-restores, before applying those parameter group changes to your production DB instances.

Example using the DB parameter function GREATEST

You can specify the GREATEST function in an Oracle processes parameter. Use it to set the number of user processes to the larger of either 80 or DBInstanceClassMemory divided by 9,868,951.

```
GREATEST({DBInstanceClassMemory/9868951},80)
```

Example using the DB parameter function LEAST

You can specify the LEAST function in a MySQL max_binlog_cache_size parameter value. Use it to set the maximum cache size a transaction can use in a MySQL instance to the lesser of 1 MB or DBInstanceClass/256.

```
LEAST({DBInstanceClassMemory/256},10485760)
```

Managing an Amazon RDS DB instance

Following, you can find instructions for managing and maintaining your Amazon RDS DB instance.

Topics

- [Stopping an Amazon RDS DB instance temporarily \(p. 317\)](#)
- [Starting an Amazon RDS DB instance that was previously stopped \(p. 320\)](#)
- [Connecting an EC2 instance and an RDS database automatically \(p. 321\)](#)
- [Modifying an Amazon RDS DB instance \(p. 327\)](#)
- [Modifying a Multi-AZ DB cluster \(p. 341\)](#)
- [Maintaining a DB instance \(p. 350\)](#)
- [Upgrading a DB instance engine version \(p. 360\)](#)
- [Renaming a DB instance \(p. 364\)](#)
- [Rebooting a DB instance \(p. 366\)](#)
- [Rebooting Multi-AZ DB clusters and reader DB instances \(p. 368\)](#)
- [Working with read replicas \(p. 370\)](#)
- [Tagging Amazon RDS resources \(p. 392\)](#)
- [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#)
- [Working with storage for Amazon RDS DB instances \(p. 410\)](#)
- [Deleting a DB instance \(p. 421\)](#)
- [Deleting a Multi-AZ DB cluster \(p. 424\)](#)

Stopping an Amazon RDS DB instance temporarily

Suppose that you use a DB instance intermittently, for temporary testing, or for a daily development activity. If so, you can stop your Amazon RDS DB instance temporarily to save money. While your DB instance is stopped, you are charged for provisioned storage (including Provisioned IOPS). You're also charged for backup storage, including manual snapshots and automated backups within your specified retention window. However, you're not charged for DB instance hours. For more information, see [Billing FAQs](#).

Note

In some cases, a large amount of time is required to stop a DB instance. If you want to stop your DB instance and restart it immediately, you can reboot the DB instance. For information about rebooting a DB instance, see [Rebooting a DB instance \(p. 366\)](#).

You can stop and start DB instances that are running the following engines:

- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

Stopping and starting a DB instance is supported for all DB instance classes, and in all AWS Regions.

You can stop and start a DB instance whether it is configured for a single Availability Zone. Or you can do so or for Multi-AZ, for database engines that support Multi-AZ deployments. You can't stop an Amazon RDS for SQL Server DB instance in a Multi-AZ configuration.

Note

For a Multi-AZ deployment, a large amount of time might be required to stop a DB instance.

If you have at least one backup after a previous failover, then you can speed up the stop DB instance operation. To do so, perform a reboot with failover operation before stopping the DB instance.

When you stop a DB instance, the DB instance performs a normal shutdown and stops running. The status of the DB instance changes to stopping and then stopped. Occasionally, an RDS for PostgreSQL DB instance doesn't shut down cleanly. If this happens, you see that the instance goes through a recovery process when you restart it later. This is expected behavior of the database engine, intended to protect database integrity. Some memory-based statistics and counters don't retain history and are re-initialized after restart, to capture the operational workload moving forward.

At the end of the normal shutdown process, any storage volumes remain attached to the DB instance, and their data is kept. Any data stored in the RAM of the DB instance is deleted.

Stopping a DB instance removes pending actions, except for pending actions for the DB instance's option group or DB parameter group.

Automated backups aren't created while a DB instance is stopped. Backups can be retained longer than the backup retention period if a DB instance has been stopped. RDS doesn't include time spent in the stopped state when the backup retention window is calculated.

Important

You can stop a DB instance for up to seven days. If you don't manually start your DB instance after seven days, your DB instance is automatically started. This way, it doesn't fall behind any required maintenance updates.

Benefits

Stopping and starting a DB instance is faster than creating a DB snapshot, and then restoring the snapshot.

When you stop a DB instance it retains its ID, Domain Name Server (DNS) endpoint, parameter group, security group, and option group. When you start a DB instance, it has the same configuration as when you stopped it. In addition, if you stop a DB instance, Amazon RDS keeps the Amazon S3 transaction logs. This means that you can do a point-in-time restore if necessary.

Limitations

The following are some limitations to stopping and starting a DB instance:

- You can't stop a DB instance that has a read replica, or that is a read replica.
- You can't stop an Amazon RDS for SQL Server DB instance in a Multi-AZ configuration.
- You can't modify a stopped DB instance.
- You can't delete an option group that is associated with a stopped DB instance.
- You can't delete a DB parameter group that is associated with a stopped DB instance.
- In a Multi-AZ configuration, the primary and secondary Availability Zones might be switched after you start the DB instance.

Option and parameter group considerations

You can't remove persistent options (including permanent options) from an option group if there are DB instances associated with that option group. This functionality is also true of any DB instance with a state of stopping, stopped, or starting.

You can change the option group or DB parameter group that is associated with a stopped DB instance. However, the change doesn't occur until the next time you start the DB instance. If you chose to apply changes immediately, the change occurs when you start the DB instance. Otherwise the change occurs during the next maintenance window after you start the DB instance.

Public IP address

When you stop a DB instance, it retains its DNS endpoint. If you stop a DB instance that has a public IP address, Amazon RDS releases its public IP address. When the DB instance is restarted, it has a different public IP address.

Note

You should always connect to a DB instance using the DNS endpoint, not the IP address.

Stopping a DB instance temporarily

You can stop a DB using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To stop a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to stop.

3. For **Actions**, choose **Stop**.
4. (Optional) In the **Stop DB Instance** window, choose **Yes** for **Create Snapshot?** and enter the snapshot name for **Snapshot name**. Choose **Yes** if you want to create a snapshot of the DB instance before stopping it.
5. Choose **Yes, Stop Now** to stop the DB instance, or choose **Cancel** to cancel the operation.

AWS CLI

To stop a DB instance by using the AWS CLI, call the [stop-db-instance](#) command with the following option:

- `--db-instance-identifier` – the name of the DB instance.

Example

```
aws rds stop-db-instance --db-instance-identifier mydbinstance
```

RDS API

To stop a DB instance by using the Amazon RDS API, call the [StopDBInstance](#) operation with the following parameter:

- `DBInstanceIdentifier` – the name of the DB instance.

Starting an Amazon RDS DB instance that was previously stopped

You can stop your Amazon RDS DB instance temporarily to save money. After you stop your DB instance, you can restart it to begin using it again. For more details about stopping and starting DB instances, see [Stopping an Amazon RDS DB instance temporarily \(p. 317\)](#).

When you start a DB instance that you previously stopped, the DB instance retains certain information. This information is the ID, Domain Name Server (DNS) endpoint, parameter group, security group, and option group. When you start a stopped instance, you are charged a full instance hour.

Console

To start a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to start.
3. For **Actions**, choose **Start**.

AWS CLI

To start a DB instance by using the AWS CLI, call the `start-db-instance` command with the following option:

- `--db-instance-identifier` – The name of the DB instance.

Example

```
aws rds start-db-instance --db-instance-identifier mydbinstance
```

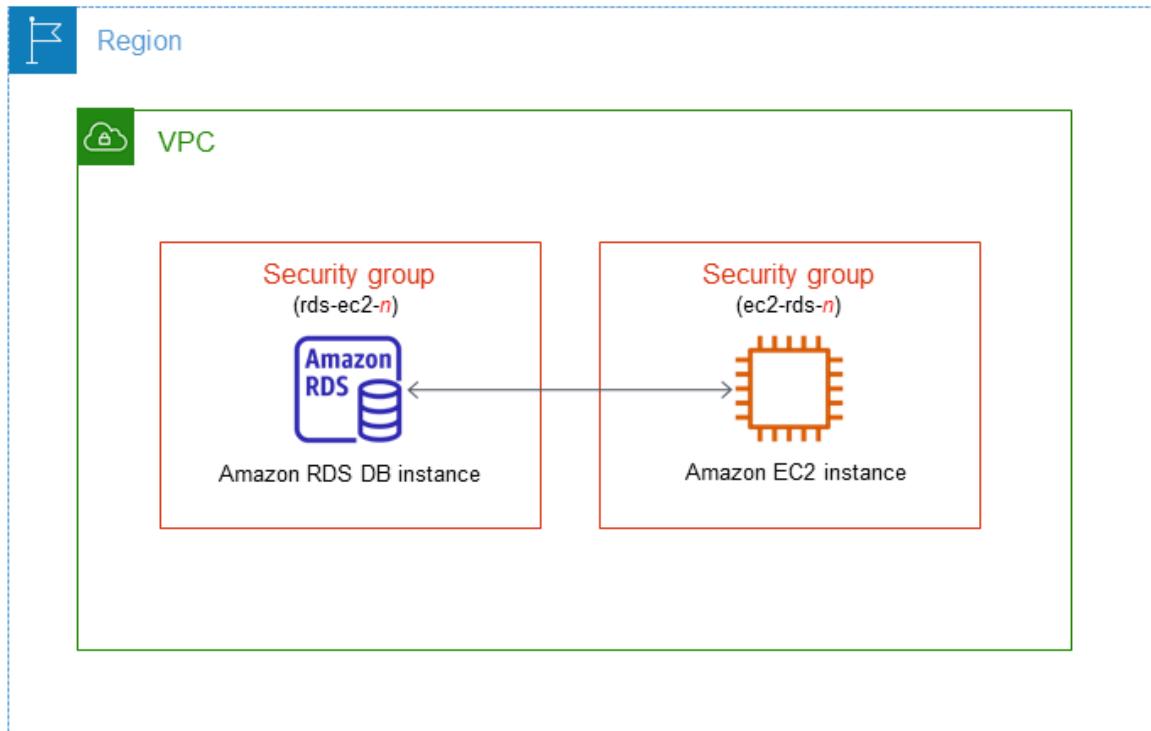
RDS API

To start a DB instance by using the Amazon RDS API, call the `StartDBInstance` operation with the following parameter:

- `DBInstanceIdentifier` – The name of the DB instance.

Connecting an EC2 instance and an RDS database automatically

You can use the RDS console to simplify setting up a connection between an EC2 instance and an RDS database. The RDS database can be a DB instance or a Multi-AZ DB cluster.



Topics

- [Overview of automatic connectivity with an EC2 instance \(p. 321\)](#)
- [Connecting an EC2 instance and an RDS database automatically \(p. 324\)](#)
- [Viewing connecting compute resources \(p. 326\)](#)

Overview of automatic connectivity with an EC2 instance

When you set up a connection between an EC2 instance and an RDS database automatically, RDS configures the VPC security group for your EC2 instance and for your RDS database.

The following are requirements for connecting an EC2 instance with an RDS database:

- The EC2 instance must exist in the same VPC as the RDS database.
If no EC2 instances exist in the same VPC, the console provides a link to create one.
- The user who is setting up connectivity must have permissions to perform the following EC2 operations:
 - `ec2:AuthorizeSecurityGroupEgress`
 - `ec2:AuthorizeSecurityGroupIngress`

- ec2:CreateSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:ModifyNetworkInterfaceAttribute
- ec2:RevokeSecurityGroupEgress

If the DB instance and EC2 instance are in different Availability Zones, there is the possibility of cross Availability Zone costs.

When you set up a connection to an EC2 instance, RDS takes an action based on the current configuration of the security groups associated with the RDS database and EC2 instance, as described in the following table.

Current RDS security group configuration	Current EC2 security group configuration	RDS action
There are one or more security groups associated with the RDS database with a name that matches the pattern <code>rds-ec2-<i>n</i></code> (where <i>n</i> is a number). A security group that matches the pattern hasn't been modified. This security group has only one inbound rule with the VPC security group of the EC2 instance as the source.	There are one or more security groups associated with the EC2 instance with a name that matches the pattern <code>rds-ec2-<i>n</i></code> (where <i>n</i> is a number). A security group that matches the pattern hasn't been modified. This security group has only one outbound rule with the VPC security group of the RDS database as the source.	RDS takes no action. A connection was already configured automatically between the EC2 instance and RDS database. Because a connection already exists between the EC2 instance and the RDS database, the security groups aren't modified.
Either of the following conditions apply: <ul style="list-style-type: none"> • There is no security group associated with the RDS database with a name that matches the pattern <code>rds-ec2-<i>n</i></code>. • There are one or more security groups associated with the RDS database with a name that matches the pattern <code>rds-ec2-<i>n</i></code>. However, none of these security groups can be used for the connection with the EC2 instance. A security group can't be used if it doesn't have one inbound rule with the VPC security group of the EC2 instance as the source. A security group also can't be used if it has been modified. Examples of modifications include adding a rule or changing the port of an existing rule. 	Either of the following conditions apply: <ul style="list-style-type: none"> • There is no security group associated with the EC2 instance with a name that matches the pattern <code>ec2-rds-<i>n</i></code>. • There are one or more security groups associated with the EC2 instance with a name that matches the pattern <code>ec2-rds-<i>n</i></code>. However, none of these security groups can be used for the connection with the RDS database. A security group can't be used if it doesn't have one outbound rule with the VPC security group of the RDS database as the source. A security group also can't be used if it has been modified. 	RDS action: create new security groups
There are one or more security groups associated with the RDS database with a name that matches	There are one or more security groups associated with the EC2 instance with a name that matches	RDS action: create new security groups

Current RDS security group configuration	Current EC2 security group configuration	RDS action
the pattern <code>rds-ec2-n</code> . A security group that matches the pattern hasn't been modified. This security group has only one inbound rule with the VPC security group of the EC2 instance as the source.	the pattern <code>ec2-rds-n</code> . However, none of these security groups can be used for the connection with the RDS database. A security group can't be used if it doesn't have one outbound rule with the VPC security group of the RDS database as the source. A security group also can't be used if it has been modified.	
There are one or more security groups associated with the RDS database with a name that matches the pattern <code>rds-ec2-n</code> . A security group that matches the pattern hasn't been modified. This security group has only one inbound rule with the VPC security group of the EC2 instance as the source.	A valid EC2 security group for the connection exists, but it is not associated with the EC2 instance. This security group has a name that matches the pattern <code>rds-ec2-n</code> . It hasn't been modified. It has only one outbound rule with the VPC security group of the RDS database as the source.	RDS action: associate EC2 security group
Either of the following conditions apply: <ul style="list-style-type: none"> • There is no security group associated with the RDS database with a name that matches the pattern <code>rds-ec2-n</code>. • There are one or more security groups associated with the RDS database with a name that matches the pattern <code>rds-ec2-n</code>. However, none of these security groups can be used for the connection with the EC2 instance. A security group can't be used if it doesn't have one inbound rule with the VPC security group of the EC2 instance as the source. A security group also can't be used if it has been modified. 	There are one or more security groups associated with the EC2 instance with a name that matches the pattern <code>rds-ec2-n</code> . A security group that matches the pattern hasn't been modified. This security group has only one outbound rule with the VPC security group of the RDS database as the source.	RDS action: create new security groups

RDS action: create new security groups

RDS takes the following actions:

- Creates a new security group that matches the pattern `rds-ec2-n`. This security group has an inbound rule with the VPC security group of the EC2 instance as the source. This security group is associated with the RDS database and allows the EC2 instance to access the RDS database.
- Creates a new security group that matches the pattern `ec2-rds-n`. This security group has an outbound rule with the VPC security group of the RDS database as the source. This security group is associated with the EC2 instance and allows the EC2 instance to send traffic to the RDS database.

RDS action: associate EC2 security group

RDS associates the valid, existing EC2 security group with the EC2 instance. This security group allows the EC2 instance to send traffic to the RDS database.

Connecting an EC2 instance and an RDS database automatically

Before setting up a connection between an EC2 instance and an RDS database, make sure you meet the requirements described in [Overview of automatic connectivity with an EC2 instance \(p. 321\)](#).

If you change these security groups after you configure connectivity, the changes might affect the connection between the EC2 instance and the RDS database.

Note

You can only set up a connection between an EC2 instance and an RDS database automatically by using the AWS Management Console. You can't set up a connection automatically with the AWS CLI or RDS API.

To connect an EC2 instance and an RDS database automatically

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS database.
3. For **Actions**, choose **Set up EC2 connection**.

The **Set up EC2 connection** page appears.

The screenshot shows the 'Set up EC2 connection' page. At the top, it says 'Select EC2 instance'. Below that, under 'Database', it shows 'database-mysql'. Under 'EC2 instance', it says 'Choose the EC2 instance to connect to this database. Only EC2 instances in the same VPC as the database are shown. If no EC2 instances in the same VPC are available, you can create a new EC2 instance.' A dropdown menu is open, showing 'ec2-instance-name us-east-1a'. To the right of the dropdown is a 'Create EC2 instance' button with a plus sign icon. At the bottom right of the page are 'Cancel' and 'Continue' buttons.

4. On the **Set up EC2 connection** page, choose the EC2 instance.

If no EC2 instances exist in the same VPC, choose **Create EC2 instance** to create one. In this case, make sure the new EC2 instance is in the same VPC as the RDS database.

5. Choose **Continue**.

The **Review and confirm** page appears.

Review and confirm

Connection summary Info

You are setting up a connection between RDS database [database-mysql](#) and EC2 instance [i-123456789](#). 

To set up a connection between the database and the EC2 instance, VPC security group <name> is added to the database, and VPC security group <name> is added to the EC2 instance.



Bold indicates an addition being made to set up a connection.

Changes to RDS database: database-mysql

Attribute	Current value	New value
Security group	default	default, rds-ec2-1

Changes to EC2 instance: i-123456789

Attribute	Current value	New value
Security group	default	default, ec2-rds-1

[Cancel](#)

[Previous](#)

[Set up connection](#)

- On the **Review and confirm** page, review the changes that RDS will make to set up connectivity with the EC2 instance.

If the changes are correct, choose **Set up connection**.

If the changes aren't correct, choose **Previous** or **Cancel**.

Viewing connecting compute resources

You can use the AWS Management Console to view the compute resources that are connected to an RDS database. The resources shown include compute resource connections that were set up automatically. You can set up connectivity with compute resources automatically in the following ways:

- You can select the compute resource when you create the database.

For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#) and [Creating a Multi-AZ DB cluster \(p. 252\)](#).

- You can set up connectivity between an existing database and a compute resource.

For more information, see [Connecting an EC2 instance and an RDS database automatically \(p. 324\)](#).

The listed compute resources don't include ones that were connected to the database manually. For example, you can allow a compute resource to access a database manually by adding a rule to the VPC security group associated with the database.

For a compute resource to be listed, the following conditions must apply:

- The name of the security group associated with the compute resource matches the pattern `ec2-rds-n` (where `n` is a number).
- The security group associated with the compute resource has an outbound rule with the port range set to the port used by the RDS database.
- The security group associated with the compute resource has an outbound rule with the source set to a security group associated with the RDS database.
- The name of the security group associated with the RDS database matches the pattern `rds-ec2-n` (where `n` is a number).
- The security group associated with the RDS database has an inbound rule with the port range set to the port used by the RDS database.
- The security group associated with the RDS database has an inbound rule with the source set to a security group associated with the compute resource.

To connect an EC2 instance and an RDS database automatically

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the name of the RDS database.
3. On the **Connectivity & security** tab, view the compute resources in the **Connected compute resources**.

Connected compute resources (1) Info				
Connections to compute resources that were created automatically by RDS are shown here. Connections to compute resources that were created manually aren't shown.				
<input type="text"/> Filter by compute resources < 1 > 				
Resource identifier	Resource type	Availability zone	RDS security group	Compute resource security group
i-000000000000000000	EC2 Instance	us-west-1b	rds-ec2-1	ec2-rds-1

Modifying an Amazon RDS DB instance

You can change the settings of a DB instance to accomplish tasks such as adding additional storage or changing the DB instance class. In this topic, you can find out how to modify an Amazon RDS DB instance and learn about the settings for DB instances.

We recommend that you test any changes on a test instance before modifying a production instance. Doing this helps you to fully understand the impact of each change. Testing is especially important when upgrading database versions.

Most modifications to a DB instance you can either apply immediately or defer until the next maintenance window. Some modifications, such as parameter group changes, require that you manually reboot your DB instance for the change to take effect.

Important

Some modifications result in downtime because Amazon RDS must reboot your DB instance for the change to take effect. Review the impact to your database and applications before modifying your DB instance settings.

Console

To modify a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. Change any of the settings that you want. For information about each setting, see [Settings for DB instances \(p. 328\)](#).
5. When all the changes are as you want them, choose **Continue** and check the summary of modifications.
6. (Optional) Choose **Apply immediately** to apply the changes immediately. Choosing this option can cause downtime in some cases. For more information, see [Using the Apply Immediately setting \(p. 328\)](#).
7. On the confirmation page, review your changes. If they are correct, choose **Modify DB instance** to save your changes.

Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

AWS CLI

To modify a DB instance by using the AWS CLI, call the `modify-db-instance` command. Specify the DB instance identifier and the values for the options that you want to modify. For information about each option, see [Settings for DB instances \(p. 328\)](#).

Example

The following code modifies `mydbinstance` by setting the backup retention period to 1 week (7 days). The code enables deletion protection by using `--deletion-protection`. To disable deletion protection, use `--no-deletion-protection`. The changes are applied during the next maintenance window by using `--no-apply-immediately`. Use `--apply-immediately` to apply the changes immediately. For more information, see [Using the Apply Immediately setting \(p. 328\)](#).

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
  --db-instance-identifier mydbinstance \  
  --backup-retention-period 7 \  
  --deletion-protection \  
  --no-apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^  
  --db-instance-identifier mydbinstance ^  
  --backup-retention-period 7 ^  
  --deletion-protection ^  
  --no-apply-immediately
```

RDS API

To modify a DB instance by using the Amazon RDS API, call the [ModifyDBInstance](#) operation. Specify the DB instance identifier, and the parameters for the settings that you want to modify. For information about each parameter, see [Settings for DB instances \(p. 328\)](#).

Using the Apply Immediately setting

When you modify a DB instance, you can apply the changes immediately. To apply changes immediately, you choose the **Apply Immediately** option in the AWS Management Console. Or you use the `--apply-immediately` parameter when calling the AWS CLI or set the `ApplyImmediately` parameter to `true` when using the Amazon RDS API.

If you don't choose to apply changes immediately, the changes are put into the pending modifications queue. During the next maintenance window, any pending changes in the queue are applied. If you choose to apply changes immediately, your new changes and any changes in the pending modifications queue are applied.

Important

If any of the pending modifications require the DB instance to be temporarily unavailable (*downtime*), choosing the apply immediately option can cause unexpected downtime.

When you choose to apply a change immediately, any pending modifications are also applied immediately, instead of during the next maintenance window.

If you don't want a pending change to be applied in the next maintenance window, you can modify the DB instance to revert the change. You can do this by using the AWS CLI and specifying the `--apply-immediately` option.

Changes to some database settings are applied immediately, even if you choose to defer your changes. To see how the different database settings interact with the apply immediately setting, see [Settings for DB instances \(p. 328\)](#).

Settings for DB instances

In the following table, you can find details about which settings you can and can't modify. You can also find when changes can be applied and whether the changes cause downtime for your DB instance. By using Amazon RDS features such as Multi-AZ, you can minimize downtime if you later modify the DB instance. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

You can modify a DB instance using the console, the `modify-db-instance` CLI command, or the `ModifyDBInstance` RDS API operation.

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
<p>Allocated storage</p> <p>The storage, in gibibytes, that you want to allocate for your DB instance. You can only increase the allocated storage. You can't reduce the allocated storage.</p> <p>You can't modify the storage of some older DB instances, or DB instances restored from older DB snapshots. The Allocated storage setting is disabled in the console if your DB instance isn't eligible. You can check whether you can allocate more storage by using the CLI command describe-valid-db-instance-modifications. This command returns the valid storage options for your DB instance.</p> <p>You can't modify allocated storage if the DB instance status is storage-optimization. You also can't modify allocated storage for a DB instance if it's been modified in the last six hours.</p> <p>The maximum storage allowed depends on your DB engine and the storage type. For more information, see Amazon RDS DB instance storage (p. 64).</p>	<p>CLI option: --allocated-storage</p> <p>RDS API parameter: AllocatedStorage</p>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	<p>Downtime doesn't occur during this change. Performance might be degraded during the change.</p>	All DB engines
<p>Auto minor version upgrade</p> <p>Yes to enable your DB instance to receive preferred minor DB engine version upgrades automatically when they become available. Amazon RDS performs automatic minor version upgrades in the maintenance window. Otherwise, No.</p> <p>For more information, see Automatically upgrading the minor engine version (p. 362).</p>	<p>CLI option: --auto-minor-version-upgrade --no-auto-minor-version-upgrade</p> <p>RDS API parameter: AutoMinorVersionUpgrade</p>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Backup replication <p>Choose Enable replication to another AWS Region to create backups in an additional Region for disaster recovery.</p> <p>Then choose the Destination Region for the additional backups.</p>	Not available when modifying a DB instance. For information on enabling cross-Region backups using the AWS CLI or RDS API, see Enabling cross-Region automated backups (p. 439) .	The change is applied asynchronously, as soon as possible.	Downtime doesn't occur during this change.	Oracle, PostgreSQL, SQL Server
Backup retention period <p>The number of days that automatic backups are retained. To disable automatic backups, set the backup retention period to 0.</p> <p>For more information, see Working with backups (p. 427).</p> <p>Note If you use AWS Backup to manage your backups, this option doesn't appear. For information about AWS Backup, see the AWS Backup Developer Guide.</p>	CLI option: <code>--backup-retention-period</code> RDS API parameter: <code>BackupRetentionPeriod</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, and you change the setting from a nonzero value to another nonzero value, the change is applied asynchronously, as soon as possible. Otherwise, the change occurs during the next maintenance window.	Downtime occurs if you change from 0 to a nonzero value, or from a nonzero value to 0. This applies to both Single-AZ and Multi-AZ DB instances.	All DB engines
Backup window <p>The time range during which automated backups of your databases occur. The backup window is a start time in Universal Coordinated Time (UTC), and a duration in hours.</p> <p>For more information, see Working with backups (p. 427).</p> <p>Note If you use AWS Backup to manage your backups, this option doesn't appear. For information about AWS Backup, see the AWS Backup Developer Guide.</p>	CLI option: <code>--preferred-backup-window</code> RDS API parameter: <code>PreferredBackupWindow</code>	The change is applied asynchronously, as soon as possible.	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Certificate authority The certificate that you want to use for SSL/TLS connections. For more information, see Using SSL/TLS to encrypt a connection to a DB instance (p. 2005) .	CLI option: <code>--ca-certificate-identifier</code> RDS API parameter: <code>CACertificateIdentifier</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime occurs during this change.	All DB engines
Copy tags to snapshots If you have any DB instance tags, enable this option to copy them when you create a DB snapshot. For more information, see Tagging Amazon RDS resources (p. 392) .	CLI option: <code>--copy-tags-to-snapshot</code> or <code>--no-copy-tags-to-snapshot</code> RDS API parameter: <code>CopyTagsToSnapshot</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
Database port The port that you want to use to access the DB instance. The port value must not match any of the port values specified for options in the option group that is associated with the DB instance. For more information, see Connecting to an Amazon RDS DB instance (p. 267) .	CLI option: <code>--db-port-number</code> RDS API parameter: <code>DBPortNumber</code>	The change occurs immediately. This setting ignores the apply immediately setting.	The DB instance is rebooted immediately.	All DB engines
DB engine version The version of the DB engine that you want to use. Before you upgrade your production DB instance, we recommend that you test the upgrade process on a test DB instance. Doing this helps verify its duration and validate your applications. For more information, see Upgrading a DB instance engine version (p. 360) .	CLI option: <code>--engine-version</code> RDS API parameter: <code>EngineVersion</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime occurs during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
DB instance class The DB instance class that you want to use. For more information, see DB instance classes (p. 10) .	CLI option: <code>--db-instance-class</code> RDS API parameter: <code>DBInstanceClass</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime occurs during this change.	All DB engines
DB instance identifier The new DB instance identifier. This value is stored as a lowercase string. For more information about the effects of renaming a DB instance, see Renaming a DB instance (p. 364) .	CLI option: <code>--new-db-instance-identifier</code> RDS API parameter: <code>NewDBInstanceIdentifier</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime occurs during this change.	All DB engines
DB parameter group The DB parameter group that you want associated with the DB instance. For more information, see Working with parameter groups (p. 289) .	CLI option: <code>--db-parameter-group-name</code> RDS API parameter: <code>DBParameterGroupName</code>	The parameter group change occurs immediately.	Downtime doesn't occur during this change. When you associate a new DB parameter group with a DB instance, the modified static and dynamic parameters are applied only after the DB instance is rebooted. However, if you modify dynamic parameters in the newly associated DB parameter group, these changes are applied immediately without a reboot. For more information, see Working with parameter groups (p. 289) and Rebooting a DB instance (p. 366) .	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Deletion protection Enable deletion protection to prevent your DB instance from being deleted. For more information, see Deleting a DB instance (p. 421) .	CLI option: <code>--deletion-protection --no-deletion-protection</code> RDS API parameter: <code>DeletionProtection</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
Enhanced Monitoring Enable Enhanced Monitoring to enable gathering metrics in real time for the operating system that your DB instance runs on. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) .	CLI option: <code>--monitoring-interval and --monitoring-role-arn</code> RDS API parameter: <code>MonitoringInterval</code> and <code>MonitoringRoleArn</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
IAM DB authentication Enable IAM DB authentication to authenticate database users through IAM users and roles. For more information, see IAM database authentication for MariaDB, MySQL, and PostgreSQL (p. 2048) .	CLI option: <code>--enable-iam-database-authentication --no-enable-iam-database-authentication</code> RDS API parameter: <code>EnableIAMDatabaseAuthentication</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime doesn't occur during this change.	Only MariaDB, MySQL, and PostgreSQL
Kerberos authentication Choose the Active Directory to move the DB instance to. The directory must exist prior to this operation. If a directory is already selected, you can specify None to remove the DB instance from its current directory. For more information, see Kerberos authentication (p. 1999) .	CLI option: <code>--domain and --domain-iam-role-name</code> RDS API parameter: <code>Domain</code> and <code>DomainIAMRoleName</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	A brief downtime occurs during this change.	Only Microsoft SQL Server, MySQL, Oracle, and PostgreSQL

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
<p>License model</p> <p>Choose bring-your-own-license to use your license for Oracle.</p> <p>Choose license-included to use the general license agreement for Microsoft SQL Server or Oracle.</p> <p>For more information, see Licensing Microsoft SQL Server on Amazon RDS (p. 1083) and RDS for Oracle licensing options (p. 1474).</p>	CLI option: <code>--license-model</code> RDS API parameter: <code>LicenseModel</code>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	Downtime occurs during this change.	Only Microsoft SQL Server and Oracle
<p>Log exports</p> <p>The types of database log files to publish to Amazon CloudWatch Logs.</p> <p>For more information, see Publishing database logs to Amazon CloudWatch Logs (p. 683).</p>	CLI option: <code>--cloudwatch-logs-export-configuration</code> RDS API parameter: <code>CloudwatchLogsExportConfiguration</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
<p>Maintenance window</p> <p>The time range during which system maintenance occurs. System maintenance includes upgrades, if applicable. The maintenance window is a start time in Universal Coordinated Time (UTC), and a duration in hours.</p> <p>If you set the window to the current time, there must be at least 30 minutes between the current time and the end of the window. This timing helps ensure that any pending changes are applied.</p> <p>For more information, see The Amazon RDS maintenance window (p. 354).</p>	CLI option: <code>--preferred-maintenance-window</code> RDS API parameter: <code>PreferredMaintenanceWindow</code>	The change occurs immediately. This setting ignores the apply immediately setting.	If there are one or more pending actions that cause downtime, and the maintenance window is changed to include the current time, those pending actions are applied immediately and downtime occurs.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Multi-AZ deployment <p>Yes to deploy your DB instance in multiple Availability Zones. Otherwise, No.</p> <p>For more information, see Multi-AZ deployments for high availability (p. 121).</p>	CLI option: <code>--multi-az --no-multi-az</code> RDS API parameter: <code>MultiAZ</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime doesn't occur during this change. However, there is a possible performance impact. For more information, see Modifying a DB instance to be a Multi-AZ DB instance deployment (p. 123) .	All DB engines
Network type <p>The IP addressing protocols supported by the DB instance.</p> <p>IPv4 to specify that resources can communicate with the DB instance only over the Internet Protocol version 4 (IPv4) addressing protocol.</p> <p>Dual-stack mode to specify that resources can communicate with the DB instance over IPv4, Internet Protocol version 6 (IPv6), or both. Use dual-stack mode if you have any resources that must communicate with your DB instance over the IPv6 addressing protocol. Also, make sure that you associate an IPv6 CIDR block with all subnets in the DB subnet group that you specify.</p> <p>For more information, see Amazon RDS IP addressing (p. 2105).</p>	CLI option: <code>--network-type</code> RDS API parameter: <code>NetworkType</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime is possible during this change.	All DB engines
New master password <p>The password for your master user. The password must contain 8–41 alphanumeric characters.</p>	CLI option: <code>--master-user-password</code> RDS API parameter: <code>MasterUserPassword</code>	The change is applied asynchronously, as soon as possible. This setting ignores the <code>apply_immediately</code> setting.	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Option group The option group that you want associated with the DB instance. For more information, see Working with option groups (p. 273) .	CLI option: <code>--option-group-name</code> RDS API parameter: <code>OptionGroupName</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime doesn't occur during this change.	All DB engines
Performance Insights Enable Performance Insights to monitor your DB instance load so that you can analyze and troubleshoot your database performance. Performance Insights isn't available for some DB engine versions and DB instance classes. The Performance Insights section doesn't appear in the console if it isn't available for your DB instance. For more information, see Monitoring DB load with Performance Insights on Amazon RDS (p. 543) and Amazon RDS DB engine, Region, and instance class support for Performance Insights (p. 547) .	CLI option: <code>--enable-performance-insights --no-enable-performance-insights</code> RDS API parameter: <code>EnablePerformanceInsights</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
Performance Insights AWS KMS key The AWS KMS key identifier for the AWS KMS key for encryption of Performance Insights data. The key identifier is the Amazon Resource Name (ARN), AWS KMS key identifier, or the key alias for the KMS key. For more information, see Turning Performance Insights on and off (p. 549) .	CLI option: <code>--performance-insights-kms-key-id</code> RDS API parameter: <code>PerformanceInsightsKMSKeyId</code>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
<p>Performance Insights Retention period</p> <p>The amount of time, in days, to retain Performance Insights data. The retention setting in the free tier is Default (7 days). To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see Pricing and data retention for Performance Insights (p. 548).</p> <p>For more information, see Turning Performance Insights on and off (p. 549).</p>	<p>CLI option: <code>--performance-insights-retention-period</code></p> <p>RDS API parameter: <code>PerformanceInsightsRetentionPeriod</code></p>	<p>The change occurs immediately. This setting ignores the <code>apply immediately</code> setting.</p>	<p>Downtime doesn't occur during this change.</p>	All DB engines
<p>Processor features</p> <p>The number of CPU cores and the number of threads per core for the DB instance class of the DB instance.</p> <p>For more information, see Configuring the processor for a DB instance class (p. 42).</p>	<p>CLI option: <code>--processor-features</code> and <code>--use-default-processor-features</code> <code>--no-use-default-processor-features</code></p> <p>RDS API parameter: <code>ProcessorFeatures</code> and <code>UseDefaultProcessorFeatures</code></p>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	<p>Downtime occurs during this change.</p>	Only Oracle
<p>Provisioned IOPS</p> <p>The Provisioned IOPS (I/O operations per second) value for the DB instance. This setting is available only if you choose one of the following for Storage type:</p> <ul style="list-style-type: none"> • General purpose SSD (gp3) • Provisioned IOPS SSD (io1) <p>For more information, see Provisioned IOPS SSD storage (p. 66) and Amazon RDS DB instance storage (p. 64).</p>	<p>CLI option: <code>--iops</code></p> <p>RDS API parameter: <code>Iops</code></p>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	<p>Downtime doesn't occur during this change.</p>	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
<p>Public access</p> <p>Publicly accessible to give the DB instance a public IP address, meaning that it's accessible outside the VPC. To be publicly accessible, the DB instance also has to be in a public subnet in the VPC.</p> <p>Not publicly accessible to make the DB instance accessible only from inside the VPC.</p> <p>For more information, see Hiding a DB instance in a VPC from the internet (p. 2109).</p> <p>To connect to a DB instance from outside its VPC, the DB instance must be publicly accessible. Also, access must be granted using the inbound rules of the DB instance's security group. In addition, other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 2141).</p> <p>If your DB instance isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 2015).</p>	<p>CLI option: <code>--publicly-accessible --no-publicly-accessible</code></p> <p>RDS API parameter: <code>PubliclyAccessible</code></p>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
<p>Security group</p> <p>The VPC security group that you want associated with the DB instance.</p> <p>For more information, see Controlling access with security groups (p. 2085).</p>	<p>CLI option: <code>--vpc-security-group-ids</code></p> <p>RDS API parameter: <code>VpcSecurityGroupIds</code></p>	The change is applied asynchronously, as soon as possible. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
<p>Storage autoscaling</p> <p>Enable storage autoscaling to enable Amazon RDS to automatically increase storage when needed to avoid having your DB instance run out of storage space.</p> <p>Use Maximum storage threshold to set the upper limit for Amazon RDS to automatically increase storage for your DB instance. The default is 1,000 GiB.</p> <p>For more information, see Managing capacity automatically with Amazon RDS storage autoscaling (p. 412).</p>	<p>CLI option: <code>--max-allocated-storage</code></p> <p>RDS API parameter: <code>MaxAllocatedStorage</code></p>	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.	All DB engines
<p>Storage throughput</p> <p>The new storage throughput value for the DB instance. This setting is available only if you choose General purpose SSD (gp3) for Storage type.</p> <p>For more information, see Amazon RDS DB instance storage (p. 64).</p>	<p>CLI option: <code>--storage-throughput</code></p> <p>RDS API parameter: <code>StorageThroughput</code></p>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	Downtime doesn't occur during this change.	All DB engines

Console setting and description	CLI option and RDS API parameter	When the change occurs	Downtime notes	Supported DB engines
Storage type The storage type that you want to use. If you choose General Purpose SSD (gp3) , you can provision additional Provisioned IOPS and Storage throughput under Advanced settings . If you choose Provisioned IOPS SSD (io1) , enter the Provisioned IOPS value. After Amazon RDS begins to modify your DB instance to change the storage size or type, you can't submit another request to change the storage size, performance, or type for six hours. For more information, see Amazon RDS storage types (p. 64) .	CLI option: <code>--storage-type</code> RDS API parameter: <code>StorageType</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	The following changes all result in a brief downtime while the process starts. After that, you can use your database normally while the change takes place. <ul style="list-style-type: none"> • From General Purpose (SSD) or Provisioned IOPS (SSD) to Magnetic. • From Magnetic to General Purpose (SSD) or Provisioned IOPS (SSD). 	All DB engines
DB subnet group The DB subnet group for the DB instance. You can use this setting to move your DB instance to a different VPC. For more information, see Amazon VPC VPCs and Amazon RDS (p. 2103) .	CLI option: <code>--db-subnet-group-name</code> RDS API parameter: <code>DBSubnetGroupName</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime occurs during this change.	All DB engines

Modifying a Multi-AZ DB cluster

A Multi-AZ DB cluster has a writer DB instance and two reader DB instances in three separate Availability Zones. Multi-AZ DB clusters provide high availability, increased capacity for read workloads, and lower latency when compared to Multi-AZ deployments. For more information about Multi-AZ DB clusters, see [Multi-AZ DB cluster deployments \(p. 127\)](#).

You can modify a Multi-AZ DB cluster to change its settings. You can also perform operations on a Multi-AZ DB cluster, such as taking a snapshot of it. However, you can't modify the DB instances in a Multi-AZ DB cluster, and the only supported operation is rebooting a DB instance.

Note

Multi-AZ DB clusters are supported only for the MySQL and PostgreSQL DB engines.

You can modify a Multi-AZ DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To modify a Multi-AZ DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the Multi-AZ DB cluster that you want to modify.
3. Choose **Modify**. The **Modify DB cluster** page appears.
4. Change any of the settings that you want. For information about each setting, see [Settings for modifying Multi-AZ DB clusters \(p. 342\)](#).
5. When all the changes are as you want them, choose **Continue** and check the summary of modifications.
6. (Optional) Choose **Apply immediately** to apply the changes immediately. Choosing this option can cause downtime in some cases. For more information, see [Using the Apply Immediately setting \(p. 342\)](#).
7. On the confirmation page, review your changes. If they're correct, choose **Modify DB cluster** to save your changes.

Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

AWS CLI

To modify a Multi-AZ DB cluster by using the AWS CLI, call the `modify-db-cluster` command. Specify the DB cluster identifier and the values for the options that you want to modify. For information about each option, see [Settings for modifying Multi-AZ DB clusters \(p. 342\)](#).

Example

The following code modifies `my-multi-az-dbcluster` by setting the backup retention period to 1 week (7 days). The code turns on deletion protection by using `--deletion-protection`. To turn off deletion protection, use `--no-deletion-protection`. The changes are applied during the next maintenance window by using `--no-apply-immediately`. Use `--apply-immediately` to apply the changes immediately. For more information, see [Using the Apply Immediately setting \(p. 342\)](#).

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier my-multi-az-dbcluster \
    --backup-retention-period 7 \
```

```
--deletion-protection \
--no-apply-immediately
```

For Windows:

```
aws rds modify-db-cluster ^
--db-cluster-identifier my-multi-az-dbcluster ^
--backup-retention-period 7 ^
--deletion-protection ^
--no-apply-immediately
```

RDS API

To modify a Multi-AZ DB cluster by using the Amazon RDS API, call the [ModifyDBCluster](#) operation. Specify the DB cluster identifier, and the parameters for the settings that you want to modify. For information about each parameter, see [Settings for modifying Multi-AZ DB clusters \(p. 342\)](#).

Using the Apply Immediately setting

When you modify a Multi-AZ DB cluster, you can apply the changes immediately. To apply changes immediately, you choose the **Apply Immediately** option in the AWS Management Console. Or you use the `--apply-immediately` option when calling the AWS CLI or set the `ApplyImmediately` parameter to true when using the Amazon RDS API.

If you don't choose to apply changes immediately, the changes are put into the pending modifications queue. During the next maintenance window, any pending changes in the queue are applied. If you choose to apply changes immediately, your new changes and any changes in the pending modifications queue are applied.

Important

If any of the pending modifications require the DB cluster to be temporarily unavailable (*downtime*), choosing the apply immediately option can cause unexpected downtime.

When you choose to apply a change immediately, any pending modifications are also applied immediately, instead of during the next maintenance window.

If you don't want a pending change to be applied in the next maintenance window, you can modify the DB instance to revert the change. You can do this by using the AWS CLI and specifying the `--apply-immediately` option.

Changes to some database settings are applied immediately, even if you choose to defer your changes. To see how the different database settings interact with the apply immediately setting, see [Settings for modifying Multi-AZ DB clusters \(p. 342\)](#).

Settings for modifying Multi-AZ DB clusters

For details about settings that you can use to modify a Multi-AZ DB cluster, see the following table. For more information about the AWS CLI options, see [modify-db-cluster](#). For more information about the RDS API parameters, see [ModifyDBCluster](#).

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
Allocated storage	The amount of storage to allocate for each DB instance in your DB cluster (in gibibytes).	CLI option: <code>--allocated-storage</code> API parameter:	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change	Downtime doesn't occur during this change.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
	For more information, see Amazon RDS DB instance storage (p. 64) .	AllocatedStorage	immediately, it occurs during the next maintenance window.	
Auto minor version upgrade	Enable auto minor version upgrade to have your DB cluster receive preferred minor DB engine version upgrades automatically when they become available. Amazon RDS performs automatic minor version upgrades in the maintenance window.	CLI option: --auto-minor-version-upgrade --no-auto-minor-version-upgrade API parameter: AutoMinorVersionUpgrade	The change occurs immediately. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.
Backup retention period	The number of days that you want automatic backups of your DB cluster to be retained. For any nontrivial DB cluster, set this value to 1 or greater. For more information, see Working with backups (p. 427) .	CLI option: --backup-retention-period API parameter: BackupRetentionPeriod	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, and you change the setting from a nonzero value to another nonzero value, the change is applied asynchronously, as soon as possible. Otherwise, the change occurs during the next maintenance window.	Downtime occurs if you change from 0 to a nonzero value, or from a nonzero value to 0.
Backup window	The time period during which Amazon RDS automatically takes a backup of your DB cluster. Unless you have a specific time that you want to have your database backed up, use the default of No preference . For more information, see Working with backups (p. 427) .	CLI option: --preferred-backup-window API parameter: PreferredBackupWindow	The change is applied asynchronously, as soon as possible.	Downtime doesn't occur during this change.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
Copy tags to snapshots	<p>This option copies any DB cluster tags to a DB snapshot when you create a snapshot.</p> <p>For more information, see Tagging Amazon RDS resources (p. 392).</p>	CLI option: <code>-copy-tags-to-snapshot</code> <code>-no-copy-tags-to-snapshot</code> RDS API parameter: <code>CopyTagsToSnapshot</code>	<p>The change occurs immediately. This setting ignores the apply immediately setting.</p>	Downtime doesn't occur during this change.
Database authentication	<p>For Multi-AZ DB clusters, only Password authentication is supported.</p>	<p>None because password authentication is the default.</p>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	Downtime doesn't occur during this change.
DB cluster instance class	<p>The compute and memory capacity of each DB instance in the Multi-AZ DB cluster, for example <code>db.r6gd.xlarge</code>.</p> <p>If possible, choose a DB instance class large enough that a typical query working set can be held in memory. When working sets are held in memory, the system can avoid writing to disk, which improves performance.</p> <p>Currently, Multi-AZ DB clusters only support <code>db.m6gd</code> and <code>db.r6gd</code> DB instance classes. For more information about DB instance classes, see DB instance classes (p. 10).</p>	CLI option: <code>--db-cluster-instance-class</code> RDS API parameter: <code>DBClusterInstanceClass</code>	<p>If you choose to apply the change immediately, it occurs immediately.</p> <p>If you don't choose to apply the change immediately, it occurs during the next maintenance window.</p>	Downtime occurs during this change.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
DB cluster parameter group	The DB cluster parameter group that you want associated with the DB cluster. For more information, see Working with parameter groups for Multi-AZ DB clusters (p. 133) .	CLI option: --db-cluster-parameter-group-name RDS API parameter: DBClusterParameterGroupName	The parameter group change occurs immediately.	An outage doesn't occur during this change. When you change the parameter group, changes to some parameters are applied to the DB instances in the Multi-AZ DB cluster immediately without a reboot. Changes to other parameters are applied only after the DB instances are rebooted.
DB engine version	The version of database engine that you want to use.	CLI option: --engine-version RDS API parameter: EngineVersion	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	An outage occurs during this change.
Deletion protection	Enable deletion protection to prevent your DB cluster from being deleted. For more information, see Deleting a DB instance (p. 421) .	CLI option: --deletion-protection --no-deletion-protection RDS API parameter: DeletionProtection	The change occurs immediately. This setting ignores the apply immediately setting.	An outage doesn't occur during this change.
Maintenance window	The 30-minute window in which pending modifications to your DB cluster are applied. If the time period doesn't matter, choose No preference . For more information, see The Amazon RDS maintenance window (p. 354) .	CLI option: --preferred-maintenance-window RDS API parameter: PreferredMaintenanceWindow	The change occurs immediately. This setting ignores the apply immediately setting.	If there are one or more pending actions that cause downtime, and the maintenance window is changed to include the current time, those pending actions are applied immediately and downtime occurs.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
New master password	The password for your master user account.	CLI option: <code>--master-user-password</code> RDS API parameter: <code>MasterUserPassword</code>	The change is applied asynchronously, as soon as possible. This setting ignores the apply immediately setting.	Downtime doesn't occur during this change.
Provisioned IOPS	The amount of Provisioned IOPS (input/output operations per second) to be initially allocated for the DB cluster. This setting is available only if Provisioned IOPS (io1) is selected as the storage type. For more information, see Provisioned IOPS SSD storage (p. 66) .	CLI option: <code>--iops</code> RDS API parameter: <code>Iops</code>	If you choose to apply the change immediately, it occurs immediately. If you don't choose to apply the change immediately, it occurs during the next maintenance window.	Downtime doesn't occur during this change.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
Public access	<p>Publicly accessible to give the DB cluster a public IP address, meaning that it's accessible outside its virtual private cloud (VPC). To be publicly accessible, the DB cluster also has to be in a public subnet in the VPC.</p> <p>Not publicly accessible to make the DB cluster accessible only from inside the VPC.</p> <p>For more information, see Hiding a DB instance in a VPC from the internet (p. 2109).</p> <p>To connect to a DB cluster from outside of its VPC, the DB cluster must be publicly accessible. Also, access must be granted using the inbound rules of the DB cluster's security group, and other requirements must be met. For more information, see Can't connect to Amazon RDS DB instance (p. 2141).</p> <p>If your DB cluster isn't publicly accessible, you can use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see Internetwork traffic privacy (p. 2015).</p>	<p>CLI option:</p> <ul style="list-style-type: none"> --publicly-accessible --no-publicly-accessible <p>RDS API parameter:</p> <ul style="list-style-type: none"> PubliclyAccessible 	The change occurs immediately. This setting ignores the apply immediately setting.	An outage doesn't occur during this change.

Console setting	Setting description	CLI option and RDS API parameter	When the change occurs	Downtime notes
VPC security group	The security groups to associate with the DB cluster. For more information, see Overview of VPC security groups (p. 2085) .	CLI option: --vpc-security-group-ids RDS API parameter: VpcSecurityGroupIds	The change is applied asynchronously, as soon as possible. This setting ignores the apply immediately setting.	An outage doesn't occur during this change.

Settings that don't apply when modifying Multi-AZ DB clusters

The following settings in the AWS CLI command [modify-db-cluster](#) and the RDS API operation [ModifyDBCluster](#) don't apply to Multi-AZ DB clusters.

You also can't modify these settings for Multi-AZ DB clusters in the console.

AWS CLI setting	RDS API setting
--allow-major-version-upgrade --no-allow-major-version-upgrade	AllowMajorVersionUpgrade
--backtrack-window	BacktrackWindow
--cloudwatch-logs-export-configuration	CloudwatchLogsExportConfiguration
--copy-tags-to-snapshot --no-copy-tags-to-snapshot	CopyTagsToSnapshot
--db-instance-parameter-group-name	DBInstanceParameterGroupName
--domain	Domain
--domain-iam-role-name	DomainIAMRoleName
--enable-global-write-forwarding --no-enable-global-write-forwarding	EnableGlobalWriteForwarding
--enable-http-endpoint --no-enable-http-endpoint	EnableHttpEndpoint
--enable-iam-database-authentication --no-enable-iam-database-authentication	EnableIAMDATABASEAuthentication
--new-db-cluster-identifier	NewDBClusterIdentifier
--option-group-name	OptionGroupName
--port	Port
--scaling-configuration	ScalingConfiguration
--storage-type	StorageType

Maintaining a DB instance

Periodically, Amazon RDS performs maintenance on Amazon RDS resources. Maintenance most often involves updates to the DB instance's underlying hardware, underlying operating system (OS), or database engine version. Updates to the operating system most often occur for security issues and should be done as soon as possible.

Some maintenance items require that Amazon RDS take your DB instance offline for a short time. Maintenance items that require a resource to be offline include required operating system or database patching. Required patching is automatically scheduled only for patches that are related to security and instance reliability. Such patching occurs infrequently (typically once every few months) and seldom requires more than a fraction of your maintenance window.

Deferred DB instance modifications that you have chosen not to apply immediately are also applied during the maintenance window. For example, you might choose to change the DB instance class or parameter group during the maintenance window. Such modifications that you specify using the **pending reboot** setting don't show up in the **Pending maintenance** list. For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Viewing pending maintenance

View whether a maintenance update is available for your DB instance by using the RDS console, the AWS CLI, or the RDS API. If an update is available, it is indicated in the **Maintenance** column for the DB instance on the Amazon RDS console, as shown following.

The screenshot shows a table in the RDS console with the following columns: Current activity, Maintenance, VPC, and Multi-AZ. There are three rows of data:

Current activity	Maintenance	VPC	Multi-AZ
0 Connections	none	vpc-2aed394c	No
0 Connections	next window	vpc-2aed394c	No
0.02 Sessions	none	vpc-2aed394c	No

If no maintenance update is available for a DB instance, the column value is **none** for it.

If a maintenance update is available for a DB instance, the following column values are possible:

- **required** – The maintenance action will be applied to the resource and can't be deferred indefinitely.
- **available** – The maintenance action is available, but it will not be applied to the resource automatically. You can apply it manually.
- **next window** – The maintenance action will be applied to the resource during the next maintenance window.
- **In progress** – The maintenance action is in the process of being applied to the resource.

If an update is available, you can take one of the actions:

- If the maintenance value is **next window**, defer the maintenance items by choosing **Defer upgrade** from **Actions**. You can't defer a maintenance action if it has already started.
- Apply the maintenance items immediately.
- Schedule the maintenance items to start during your next maintenance window.
- Take no action.

To take an action, choose the DB instance to show its details, then choose **Maintenance & backups**. The pending maintenance items appear.

The screenshot shows the 'Maintenance & backups' tab selected in the navigation bar. Under the 'Maintenance' section, it displays the status of 'Auto minor version upgrade' as 'Enabled'. The 'Pending maintenance' section shows one item: 'Automatic minor version upgrade to postgres 9.6.11', which is a 'db-upgrade' type and is set to 'next window'. There are buttons to 'Apply now' or 'Apply at next maintenance window'. A table below lists the pending maintenance item with columns for Description, Type, Status, and Apply date.

Description	Type	Status	Apply date
Automatic minor version upgrade to postgres 9.6.11	db-upgrade	next window	February 25th 2019, 3:28:00 am UTC-8 (local)

The maintenance window determines when pending operations start, but doesn't limit the total run time of these operations. Maintenance operations aren't guaranteed to finish before the maintenance window ends, and can continue beyond the specified end time. For more information, see [The Amazon RDS maintenance window \(p. 354\)](#).

You can also view whether a maintenance update is available for your DB instance by running the [describe-pending-maintenance-actions](#) AWS CLI command.

Applying updates for a DB instance

With Amazon RDS, you can choose when to apply maintenance operations. You can decide when Amazon RDS applies updates by using the RDS console, AWS Command Line Interface (AWS CLI), or RDS API.

Console

To manage an update for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that has a required update.
4. For **Actions**, choose one of the following:
 - **Upgrade now**
 - **Upgrade at next window**

Note

If you choose **Upgrade at next window** and later want to delay the update, you can choose **Defer upgrade**. You can't defer a maintenance action if it has already started. To cancel a maintenance action, modify the DB instance and disable **Auto minor version upgrade**.

AWS CLI

To apply a pending update to a DB instance, use the [apply-pending-maintenance-action](#) AWS CLI command.

Example

For Linux, macOS, or Unix:

```
aws rds apply-pending-maintenance-action \
--resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db \
--apply-action system-update \
--opt-in-type immediate
```

For Windows:

```
aws rds apply-pending-maintenance-action ^
--resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db ^
--apply-action system-update ^
--opt-in-type immediate
```

Note

To defer a maintenance action, specify `undo-opt-in` for `--opt-in-type`. You can't specify `undo-opt-in` for `--opt-in-type` if the maintenance action has already started. To cancel a maintenance action, run the [modify-db-instance](#) AWS CLI command and specify `--no-auto-minor-version-upgrade`.

To return a list of resources that have at least one pending update, use the [describe-pending-maintenance-actions](#) AWS CLI command.

Example

For Linux, macOS, or Unix:

```
aws rds describe-pending-maintenance-actions \
--resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

For Windows:

```
aws rds describe-pending-maintenance-actions ^
--resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

You can also return a list of resources for a DB instance by specifying the `--filters` parameter of the `describe-pending-maintenance-actions` AWS CLI command. The format for the `--filters` command is `Name=filter-name,Value=resource-id,...`.

The following are the accepted values for the `Name` parameter of a filter:

- `db-instance-id` – Accepts a list of DB instance identifiers or Amazon Resource Names (ARNs). The returned list only includes pending maintenance actions for the DB instances identified by these identifiers or ARNs.
- `db-cluster-id` – Accepts a list of DB cluster identifiers or ARNs for Amazon Aurora. The returned list only includes pending maintenance actions for the DB clusters identified by these identifiers or ARNs.

For example, the following example returns the pending maintenance actions for the `sample-instance1` and `sample-instance2` DB instances.

Example

For Linux, macOS, or Unix:

```
aws rds describe-pending-maintenance-actions \
--filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

For Windows:

```
aws rds describe-pending-maintenance-actions ^
--filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

RDS API

To apply an update to a DB instance, call the Amazon RDS API [ApplyPendingMaintenanceAction](#) operation.

To return a list of resources that have at least one pending update, call the Amazon RDS API [DescribePendingMaintenanceActions](#) operation.

Maintenance for Multi-AZ deployments

Running a DB instance as a Multi-AZ deployment can further reduce the impact of a maintenance event. This result is because Amazon RDS applies operating system updates by following these steps:

1. Perform maintenance on the standby.

2. Promote the standby to primary.
3. Perform maintenance on the old primary, which becomes the new standby.

When you modify the database engine for your DB instance in a Multi-AZ deployment, Amazon RDS upgrades both primary and secondary DB instances at once. In this case, the database engine for the entire Multi-AZ deployment is shut down during the upgrade.

For more information on Multi-AZ deployments, see [Multi-AZ deployments for high availability \(p. 121\)](#).

The Amazon RDS maintenance window

Every DB instance has a weekly maintenance window during which any system changes are applied. Think of the maintenance window as an opportunity to control when modifications and software patching occur. If a maintenance event is scheduled for a given week, it's initiated during the 30-minute maintenance window you identify. Most maintenance events also complete during the 30-minute maintenance window, although larger maintenance events may take more than 30 minutes to complete.

The 30-minute maintenance window is selected at random from an 8-hour block of time per region. If you don't specify a maintenance window when you create the DB instance, RDS assigns a 30-minute maintenance window on a randomly selected day of the week.

RDS consumes some of the resources on your DB instance while maintenance is being applied. You might observe a minimal effect on performance. For a DB instance, on rare occasions, a Multi-AZ failover might be required for a maintenance update to complete.

Following, you can find the time blocks for each region from which default maintenance windows are assigned.

Region Name	Region	Time Block
US East (Ohio)	us-east-2	03:00–11:00 UTC
US East (N. Virginia)	us-east-1	03:00–11:00 UTC
US West (N. California)	us-west-1	06:00–14:00 UTC
US West (Oregon)	us-west-2	06:00–14:00 UTC
Africa (Cape Town)	af-south-1	03:00–11:00 UTC
Asia Pacific (Hong Kong)	ap-east-1	06:00–14:00 UTC
Asia Pacific (Hyderabad)	ap-south-2	06:30–14:30 UTC
Asia Pacific (Jakarta)	ap-southeast-3	08:00–16:00 UTC
Asia Pacific (Mumbai)	ap-south-1	06:00–14:00 UTC
Asia Pacific (Osaka)	ap-northeast-3	22:00–23:59 UTC
Asia Pacific (Seoul)	ap-northeast-2	13:00–21:00 UTC
Asia Pacific (Singapore)	ap-southeast-1	14:00–22:00 UTC
Asia Pacific (Sydney)	ap-southeast-2	12:00–20:00 UTC

Region Name	Region	Time Block
Asia Pacific (Tokyo)	ap-northeast-1	13:00–21:00 UTC
Canada (Central)	ca-central-1	03:00–11:00 UTC
China (Beijing)	cn-north-1	06:00–14:00 UTC
China (Ningxia)	cn-northwest-1	06:00–14:00 UTC
Europe (Frankfurt)	eu-central-1	21:00–05:00 UTC
Europe (Ireland)	eu-west-1	22:00–06:00 UTC
Europe (London)	eu-west-2	22:00–06:00 UTC
Europe (Paris)	eu-west-3	23:59–07:29 UTC
Europe (Milan)	eu-south-1	02:00–10:00 UTC
Europe (Spain)	eu-south-2	02:00–10:00 UTC
Europe (Stockholm)	eu-north-1	23:00–07:00 UTC
Europe (Zurich)	eu-central-2	02:00–10:00 UTC
Middle East (Bahrain)	me-south-1	06:00–14:00 UTC
Middle East (UAE)	me-central-1	05:00–13:00 UTC
South America (São Paulo)	sa-east-1	00:00–08:00 UTC
AWS GovCloud (US-East)	us-gov-east-1	17:00–01:00 UTC
AWS GovCloud (US-West)	us-gov-west-1	06:00–14:00 UTC

Adjusting the preferred DB instance maintenance window

The maintenance window should fall at the time of lowest usage and thus might need modification from time to time. Your DB instance is unavailable during this time only if the system changes, such as a change in DB instance class, are being applied and require an outage. Your DB instance is unavailable only for the minimum amount of time required to make the necessary changes.

In the following example, you adjust the preferred maintenance window for a DB instance.

For this example, we assume that a DB instance named *mydbinstance* exists and has a preferred maintenance window of "Sun:05:00-Sun:06:00" UTC.

Console

To adjust the preferred maintenance window

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**, and then select the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB Instance** page appears.
4. In the **Maintenance** section, update the maintenance window.

Note

The maintenance window and the backup window for the DB instance cannot overlap. If you enter a value for the maintenance window that overlaps the backup window, an error message appears.

5. Choose **Continue**.

On the confirmation page, review your changes.

6. To apply the changes to the maintenance window immediately, select **Apply immediately**.
7. Choose **Modify DB Instance** to save your changes.

Alternatively, choose **Back** to edit your changes, or choose **Cancel** to cancel your changes.

AWS CLI

To adjust the preferred maintenance window, use the AWS CLI [modify-db-instance](#) command with the following parameters:

- `--db-instance-identifier`
- `--preferred-maintenance-window`

Example

The following code example sets the maintenance window to Tuesdays from 4:00-4:30AM UTC.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

RDS API

To adjust the preferred maintenance window, use the Amazon RDS API [ModifyDBInstance](#) operation with the following parameters:

- `DBInstanceIdentifier`
- `PreferredMaintenanceWindow`

Working with operating system updates

RDS for MariaDB, RDS for MySQL, and RDS for PostgreSQL DB instances occasionally require operating system updates. Amazon RDS upgrades the operating system to a newer version to improve database

performance and customers' overall security posture. Typically, the updates take about 10 minutes. Operating system updates don't change the DB engine version or DB instance class of a DB instance.

Operating system updates can be either optional or mandatory.

- An **optional update** doesn't have an apply date and can be applied at any time. While these updates are optional, we recommend that you apply them periodically to keep your RDS fleet up to date. RDS *does not* apply these updates automatically. To be notified when a new optional update becomes available, you can subscribe to [RDS-EVENT-0230 \(p. 676\)](#) in the security patching event category. For information about subscribing to RDS events, see [Subscribing to Amazon RDS event notification \(p. 655\)](#).
- A **mandatory update** is required and has an apply date. Plan to schedule your update before this date. After the specified apply date, Amazon RDS automatically upgrades the operating system for your DB instance to the latest version. The update is performed in a subsequent maintenance window for the DB instance.

Note

Staying current on all optional and mandatory updates might be required to meet various compliance obligations. We recommend that you apply all updates made available by RDS routinely during your maintenance windows.

You can use the AWS Management Console or the AWS CLI to determine whether an update is optional or mandatory.

Console

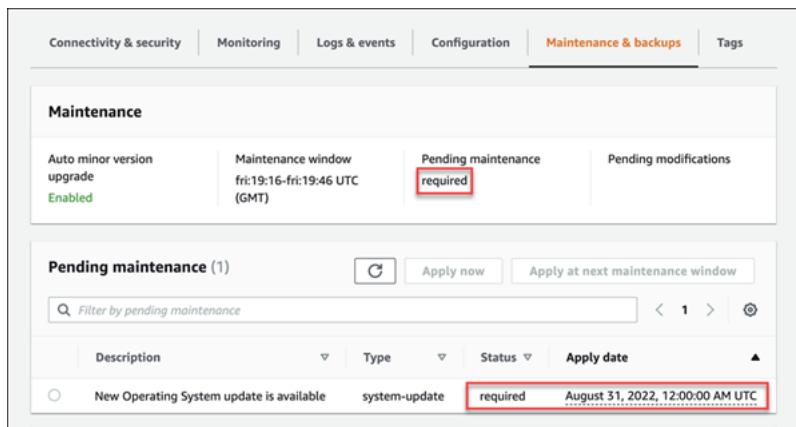
To determine whether an update is optional or mandatory using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then select the DB instance.
3. Choose **Maintenance & backups**.
4. In the **Pending maintenance** section, find the operating system update, and check the **Status** value.

In the AWS Management Console, an optional update has its maintenance **Status** set to **available** and doesn't have an **Apply date**, as shown in the following image.

Description	Type	Status	Apply date
New Operating System update is available	system-update	available	-

A mandatory update has its maintenance **Status** set to **required** and has an **Apply date**, as shown in the following image.



AWS CLI

To determine whether an update is optional or mandatory using the AWS CLI, call the [describe-pending-maintenance-actions](#) command.

```
aws rds describe-pending-maintenance-actions
```

A mandatory operating system update includes an `AutoAppliedAfterDate` value and a `CurrentApplyDate` value. An optional operating system update doesn't include these values.

The following output shows a mandatory operating system update.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb1",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "AutoAppliedAfterDate": "2022-08-31T00:00:00+00:00",
      "CurrentApplyDate": "2022-08-31T00:00:00+00:00",
      "Description": "New Operating System update is available"
    }
  ]
}
```

The following output shows an optional operating system update.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb2",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "Description": "New Operating System update is available"
    }
  ]
}
```

Availability of operating system updates

Operating system updates are specific to DB engine version and DB instance class. Therefore, DB instances receive or require updates at different times. When an operating system update is available for your DB instance based on its engine version and instance class, the update appears in the console. It can also be viewed by running AWS CLI [describe-pending-maintenance-actions](#) command or by

calling the RDS [DescribePendingMaintenanceActions](#) API operation. If an update is available for your instance, you can update your operating system by following the instructions in [Applying updates for a DB instance \(p. 352\)](#).

Mandatory operating system updates schedule

We plan to use the following schedule for mandatory operating system updates. For each date in the table, the start time is 00:00 Universal Coordinated Time (UTC).

DB engine	Apply date
RDS for MySQL	August 31, 2022*
RDS for MariaDB	August 31, 2022
RDS for PostgreSQL	August 31, 2022

* For RDS for MySQL, the date applies to the Asia Pacific (Jakarta) Region only. Mandatory operating system updates are complete for other AWS Regions.

After the apply date, Amazon RDS will automatically upgrade the operating system for your DB instances to the latest version in a subsequent maintenance window. To avoid an automatic upgrade, we recommend that you schedule your update before the apply date.

Upgrading a DB instance engine version

Amazon RDS provides newer versions of each supported database engine so you can keep your DB instance up-to-date. Newer versions can include bug fixes, security enhancements, and other improvements for the database engine. When Amazon RDS supports a new version of a database engine, you can choose how and when to upgrade your database DB instances.

There are two kinds of upgrades: major version upgrades and minor version upgrades. In general, a *major engine version upgrade* can introduce changes that are not compatible with existing applications. In contrast, a *minor version upgrade* includes only changes that are backward-compatible with existing applications.

The version numbering sequence is specific to each database engine. For example, RDS for MySQL 5.7 and 8.0 are major engine versions and upgrading from any 5.7 version to any 8.0 version is a major version upgrade. RDS for MySQL version 5.7.22 and 5.7.23 are minor versions and upgrading from 5.7.22 to 5.7.23 is a minor version upgrade.

Important

You can't modify a DB instance when it is being upgraded. During an upgrade, the DB instance status is *upgrading*.

For more information about major and minor version upgrades for a specific DB engine, see the following documentation for your DB engine:

- [Upgrading the MariaDB DB engine \(p. 998\)](#)
- [Upgrading the Microsoft SQL Server DB engine \(p. 1094\)](#)
- [Upgrading the MySQL DB engine \(p. 1343\)](#)
- [Upgrading the RDS for Oracle DB engine \(p. 1757\)](#)
- [Upgrading the PostgreSQL DB engine for Amazon RDS \(p. 1839\)](#)

For major version upgrades, you must manually modify the DB engine version through the AWS Management Console, AWS CLI, or RDS API. For minor version upgrades, you can manually modify the engine version, or you can choose to enable auto minor version upgrades.

Note

Database engine upgrades require downtime. The duration of the downtime varies based on the size of your DB instance.

Topics

- [Manually upgrading the engine version \(p. 360\)](#)
- [Automatically upgrading the minor engine version \(p. 362\)](#)

Manually upgrading the engine version

To manually upgrade the engine version of a DB instance, you can use the AWS Management Console, the AWS CLI, or the RDS API.

Console

To upgrade the engine version of a DB instance by using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to upgrade.

3. Choose **Modify**. The **Modify DB Instance** page appears.
4. For **DB engine version**, choose the new version.
5. Choose **Continue** and check the summary of modifications.
6. To apply the changes immediately, choose **Apply immediately**. Choosing this option can cause an outage in some cases. For more information, see [Using the Apply Immediately setting \(p. 328\)](#).
7. On the confirmation page, review your changes. If they are correct, choose **Modify DB Instance** to save your changes.

Alternatively, choose **Back** to edit your changes, or choose **Cancel** to cancel your changes.

AWS CLI

To upgrade the engine version of a DB instance, use the CLI `modify-db-instance` command. Specify the following parameters:

- `--db-instance-identifier` – the name of the DB instance.
- `--engine-version` – the version number of the database engine to upgrade to.

For information about valid engine versions, use the AWS CLI `describe-db-engine-versions` command.

- `--allow-major-version-upgrade` – to upgrade the major version.
- `--no-apply-immediately` – to apply changes during the next maintenance window. To apply changes immediately, use `--apply-immediately`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --engine-version new_version \
  --allow-major-version-upgrade \
  --no-apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --engine-version new_version ^
  --allow-major-version-upgrade ^
  --no-apply-immediately
```

RDS API

To upgrade the engine version of a DB instance, use the `ModifyDBInstance` action. Specify the following parameters:

- `DBInstanceIdentifier` – the name of the DB instance, for example *mydbinstance*.
- `EngineVersion` – the version number of the database engine to upgrade to. For information about valid engine versions, use the `DescribeDBEngineVersions` operation.
- `AllowMajorVersionUpgrade` – whether to allow a major version upgrade. To do so, set the value to `true`.
- `ApplyImmediately` – whether to apply changes immediately or during the next maintenance window. To apply changes immediately, set the value to `true`. To apply changes during the next maintenance window, set the value to `false`.

Automatically upgrading the minor engine version

A *minor engine version* is an update to a DB engine version within a major engine version. For example, a major engine version might be 9.6 with the minor engine versions 9.6.11 and 9.6.12 within it.

If you want Amazon RDS to upgrade the DB engine version of a database automatically, you can enable auto minor version upgrades for the database.

When Amazon RDS designates a minor engine version as the preferred minor engine version, each database that meets both of the following conditions is upgraded to the minor engine version automatically:

- The database is running a minor version of the DB engine that is lower than the preferred minor engine version.
- The database has auto minor version upgrade enabled.

You can control whether auto minor version upgrade is enabled for a DB instance when you perform the following tasks:

- [Creating a DB instance \(p. 230\)](#)
- [Modifying a DB instance \(p. 327\)](#)
- [Creating a read replica \(p. 375\)](#)
- [Restoring a DB instance from a snapshot \(p. 452\)](#)
- [Restoring a DB instance to a specific time \(p. 499\)](#)
- [Importing a DB instance from Amazon S3 \(p. 1361\)](#) (for a MySQL backup on Amazon S3)

When you perform these tasks, you can control whether auto minor version upgrade is enabled for the DB instance in the following ways:

- Using the console, set the **Auto minor version upgrade** option.
- Using the AWS CLI, set the `--auto-minor-version-upgrade` | `--no-auto-minor-version-upgrade` option.
- Using the RDS API, set the `AutoMinorVersionUpgrade` parameter.

To determine whether a maintenance update, such as a DB engine version upgrade, is available for your DB instance, you can use the console, AWS CLI, or RDS API. You can also upgrade the DB engine version manually and adjust the maintenance window. For more information, see [Maintaining a DB instance \(p. 350\)](#).

You can use the following AWS CLI command to determine the current automatic minor upgrade target version for a specified minor DB engine version in a specific AWS Region. You can find the possible `--engine` values for this command in the description for the `Engine` parameter in [CreateDBInstance](#).

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine engine \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade, EngineVersion:EngineVersion}" \
--output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine engine ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

For example, the following AWS CLI command determines the automatic minor upgrade target for MySQL minor version 8.0.11 in the US East (Ohio) AWS Region (us-east-2).

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version 8.0.11 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version 8.0.11 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Your output is similar to the following.

DescribeDBEngineVersions	
AutoUpgrade	EngineVersion
False	8.0.15
False	8.0.16
False	8.0.17
False	8.0.19
False	8.0.20
False	8.0.21
True	8.0.23
False	8.0.25

In this example, the AutoUpgrade value is True for MySQL version 8.0.23. So, the automatic minor upgrade target is MySQL version 8.0.23, which is highlighted in the output.

Important

If you plan to migrate an RDS for PostgreSQL DB instance to an Aurora PostgreSQL DB cluster soon, we strongly recommend that you turn off auto minor version upgrades for the DB instance early during planning. Migration to Aurora PostgreSQL might be delayed if the RDS for PostgreSQL version isn't yet supported by Aurora PostgreSQL. For information about Aurora PostgreSQL versions, see [Engine versions for Amazon Aurora PostgreSQL](#).

Renaming a DB instance

You can rename a DB instance by using the AWS Management Console, the AWS CLI `modify-db-instance` command, or the Amazon RDS API `ModifyDBInstance` action. Renaming a DB instance can have far-reaching effects. The following is a list of considerations before you rename a DB instance.

- When you rename a DB instance, the endpoint for the DB instance changes, because the URL includes the name you assigned to the DB instance. You should always redirect traffic from the old URL to the new one.
- When you rename a DB instance, the old DNS name that was used by the DB instance is immediately deleted, although it could remain cached for a few minutes. The new DNS name for the renamed DB instance becomes effective in about 10 minutes. The renamed DB instance is not available until the new name becomes effective.
- You cannot use an existing DB instance name when renaming an instance.
- All read replicas associated with a DB instance remain associated with that instance after it is renamed. For example, suppose you have a DB instance that serves your production database and the instance has several associated read replicas. If you rename the DB instance and then replace it in the production environment with a DB snapshot, the DB instance that you renamed will still have the read replicas associated with it.
- Metrics and events associated with the name of a DB instance are maintained if you reuse a DB instance name. For example, if you promote a read replica and rename it to be the name of the previous primary DB instance, the events and metrics associated with the primary DB instance are associated with the renamed instance.
- DB instance tags remain with the DB instance, regardless of renaming.
- DB snapshots are retained for a renamed DB instance.

Note

A DB instance is an isolated database environment running in the cloud. A DB instance can host multiple databases, or a single Oracle database with multiple schemas. For information about changing a database name, see the documentation for your DB engine.

Renaming to replace an existing DB instance

The most common reasons for renaming a DB instance are that you are promoting a read replica or you are restoring data from a DB snapshot or point-in-time recovery (PITR). By renaming the database, you can replace the DB instance without having to change any application code that references the DB instance. In these cases, you would do the following:

1. Stop all traffic going to the primary DB instance. This can involve redirecting traffic from accessing the databases on the DB instance or some other way you want to use to prevent traffic from accessing your databases on the DB instance.
2. Rename the primary DB instance to a name that indicates it is no longer the primary DB instance as described later in this topic.
3. Create a new primary DB instance by restoring from a DB snapshot or by promoting a read replica, and then give the new instance the name of the previous primary DB instance.
4. Associate any read replicas with the new primary DB instance.

If you delete the old primary DB instance, you are responsible for deleting any unwanted DB snapshots of the old primary DB instance.

For information about promoting a read replica, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Important

The DB instance is rebooted when it is renamed.

Console

To rename a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to rename.
4. Choose **Modify**.
5. In **Settings**, enter a new name for **DB instance identifier**.
6. Choose **Continue**.
7. To apply the changes immediately, choose **Apply immediately**. Choosing this option can cause an outage in some cases. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
8. On the confirmation page, review your changes. If they are correct, choose **Modify DB Instance** to save your changes.

Alternatively, choose **Back** to edit your changes, or choose **Cancel** to cancel your changes.

AWS CLI

To rename a DB instance, use the AWS CLI command `modify-db-instance`. Provide the current `--db-instance-identifier` value and `--new-db-instance-identifier` parameter with the new name of the DB instance.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier DBInstanceIdentifier \
  --new-db-instance-identifier NewDBInstanceIdentifier
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier DBInstanceIdentifier ^
  --new-db-instance-identifier NewDBInstanceIdentifier
```

RDS API

To rename a DB instance, call Amazon RDS API operation `ModifyDBInstance` with the following parameters:

- `DBInstanceIdentifier` — existing name for the instance
- `NewDBInstanceIdentifier` — new name for the instance

Rebooting a DB instance

You might need to reboot your DB instance, usually for maintenance reasons. For example, if you make certain modifications, or if you change the DB parameter group associated with the DB instance, you must reboot the instance for the changes to take effect.

Note

If a DB instance isn't using the latest changes to its associated DB parameter group, the AWS Management Console shows the DB parameter group with a status of **pending-reboot**. The **pending-reboot** parameter groups status doesn't result in an automatic reboot during the next maintenance window. To apply the latest parameter changes to that DB instance, manually reboot the DB instance. For more information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

Rebooting a DB instance restarts the database engine service. Rebooting a DB instance results in a momentary outage, during which the DB instance status is set to *rebooting*.

If the Amazon RDS DB instance is configured for Multi-AZ, you can perform the reboot with a failover. An Amazon RDS event is created when the reboot is completed. If your DB instance is a Multi-AZ deployment, you can force a failover from one Availability Zone (AZ) to another when you reboot. When you force a failover of your DB instance, Amazon RDS automatically switches to a standby replica in another Availability Zone, and updates the DNS record for the DB instance to point to the standby DB instance. As a result, you need to clean up and re-establish any existing connections to your DB instance. Rebooting with failover is beneficial when you want to simulate a failure of a DB instance for testing, or restore operations to the original AZ after a failover occurs. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Warning

When you force a failover of your DB instance, the database is abruptly interrupted. The DB instance and its client sessions might not have time to shut down gracefully. To avoid the possibility of data loss, we recommend stopping transactions on your DB instance before rebooting with a failover.

On RDS for Microsoft SQL Server, reboot with failover reboots only the primary DB instance. After the failover, the primary DB instance becomes the new secondary DB instance. Parameters might not be updated for Multi-AZ instances. For reboot without failover, both the primary and secondary DB instances reboot, and parameters are updated after the reboot. If the DB instance is unresponsive, we recommend reboot without failover.

Note

When you force a failover from one Availability Zone to another when you reboot, the Availability Zone change might not be reflected in the AWS Management Console, and in calls to the AWS CLI and RDS API, for several minutes.

You can't reboot your DB instance if it isn't in the available state. Your database can be unavailable for several reasons, such as an in-progress backup, a previously requested modification, or a maintenance-window action.

The time required to reboot your DB instance depends on the crash recovery process, database activity at the time of reboot, and the behavior of your specific DB engine. To improve the reboot time, we recommend that you reduce database activity as much as possible during the reboot process. Reducing database activity reduces rollback activity for in-transit transactions.

For a DB instance with read replicas, you can reboot the source DB instance and its read replicas independently. After a reboot completes, replication resumes automatically.

Console

To reboot a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to reboot.
3. For **Actions**, choose **Reboot**.

The **Reboot DB Instance** page appears.

4. (Optional) Choose **Reboot with failover?** to force a failover from one AZ to another.
5. Choose **Reboot** to reboot your DB instance.

Alternatively, choose **Cancel**.

AWS CLI

To reboot a DB instance by using the AWS CLI, call the `reboot-db-instance` command.

Example Simple reboot

For Linux, macOS, or Unix:

```
aws rds reboot-db-instance \
--db-instance-identifier mydbinstance
```

For Windows:

```
aws rds reboot-db-instance ^
--db-instance-identifier mydbinstance
```

Example Reboot with failover

To force a failover from one AZ to the other, use the `--force-failover` parameter.

For Linux, macOS, or Unix:

```
aws rds reboot-db-instance \
--db-instance-identifier mydbinstance \
--force-failover
```

For Windows:

```
aws rds reboot-db-instance ^
--db-instance-identifier mydbinstance ^
--force-failover
```

RDS API

To reboot a DB instance by using the Amazon RDS API, call the `RebootDBInstance` operation.

Rebooting Multi-AZ DB clusters and reader DB instances

You might need to reboot your Multi-AZ DB cluster, usually for maintenance reasons. For example, if you make certain modifications or change the DB cluster parameter group associated with a DB cluster, you reboot the DB cluster. Doing so causes the changes to take effect.

If a DB cluster isn't using the latest changes to its associated DB cluster parameter group, the AWS Management Console shows the DB cluster parameter group with a status of **pending-reboot**. The **pending-reboot** parameter groups status doesn't result in an automatic reboot during the next maintenance window. To apply the latest parameter changes to that DB cluster, manually reboot the DB cluster. For more information about parameter groups, see [Working with parameter groups for Multi-AZ DB clusters \(p. 133\)](#).

Rebooting a DB cluster restarts the database engine service. Rebooting a DB cluster results in a momentary outage, during which the DB cluster status is set to **rebooting**.

You can't reboot your DB cluster if it isn't in the **Available** state. Your database can be unavailable for several reasons, such as an in-progress backup, a previously requested modification, or a maintenance-window action.

Important

When you reboot the writer instance of a Multi-AZ DB cluster, it doesn't affect the reader DB instances in that DB cluster and no failover occurs. When you reboot a reader DB instance, no failover occurs. To fail over a Multi-AZ DB cluster, choose **Failover** in the console, call the AWS CLI command [failover-db-cluster](#), or call the API operation [FailoverDBCluster](#).

The time required to reboot your DB cluster depends on the crash recovery process, the database activity at the time of reboot, and the behavior of your specific DB cluster. To improve the reboot time, we recommend that you reduce database activity as much as possible during the reboot process. Reducing database activity reduces rollback activity for in-transit transactions.

Multi-AZ DB clusters don't support reboot with a failover.

Console

To reboot a DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the Multi-AZ DB cluster that you want to reboot.
3. For **Actions**, choose **Reboot**.

The **Reboot DB cluster** page appears.

4. Choose **Reboot** to reboot your DB cluster.

Or choose **Cancel**.

AWS CLI

To reboot a Multi-AZ DB cluster by using the AWS CLI, call the `reboot-db-cluster` command.

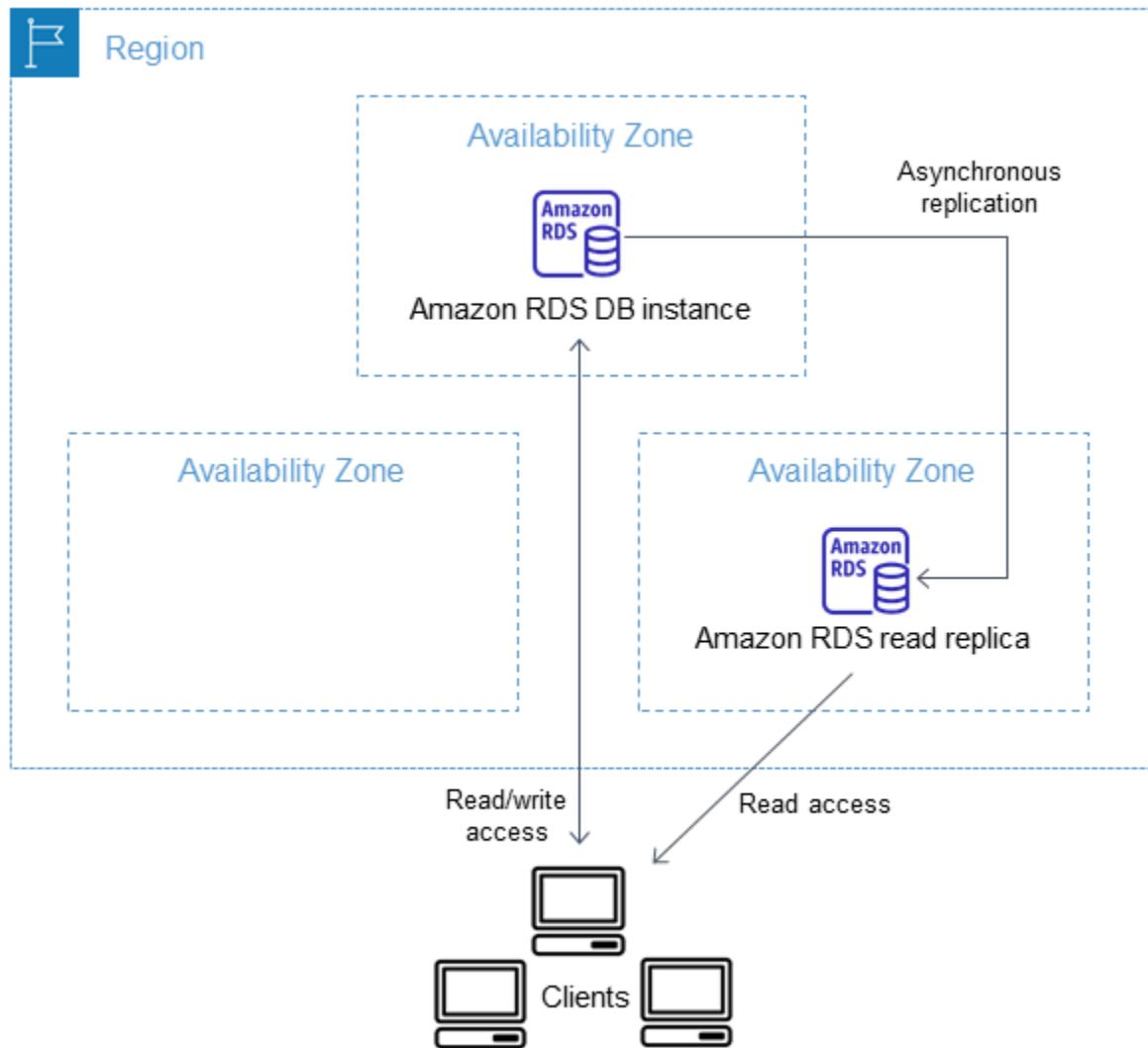
```
aws rds reboot-db-cluster --db-cluster-identifier mymultiazdbcluster
```

RDS API

To reboot a Multi-AZ DB cluster by using the Amazon RDS API, call the [RebootDBCluster](#) operation.

Working with read replicas

Amazon RDS uses the MariaDB, Microsoft SQL Server, MySQL, Oracle, and PostgreSQL DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. The source DB instance becomes the primary DB instance. Updates made to the primary DB instance are asynchronously copied to the read replica. You can reduce the load on your primary DB instance by routing read queries from your applications to the read replica. Using read replicas, you can elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.



Note

The information following applies to creating Amazon RDS read replicas either in the same AWS Region as the source DB instance, or in a separate AWS Region. The information following doesn't apply to setting up replication with an instance that is running on an Amazon EC2 instance or that is on-premises.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. Amazon RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the primary DB instance. The read replica operates as a DB instance that allows only

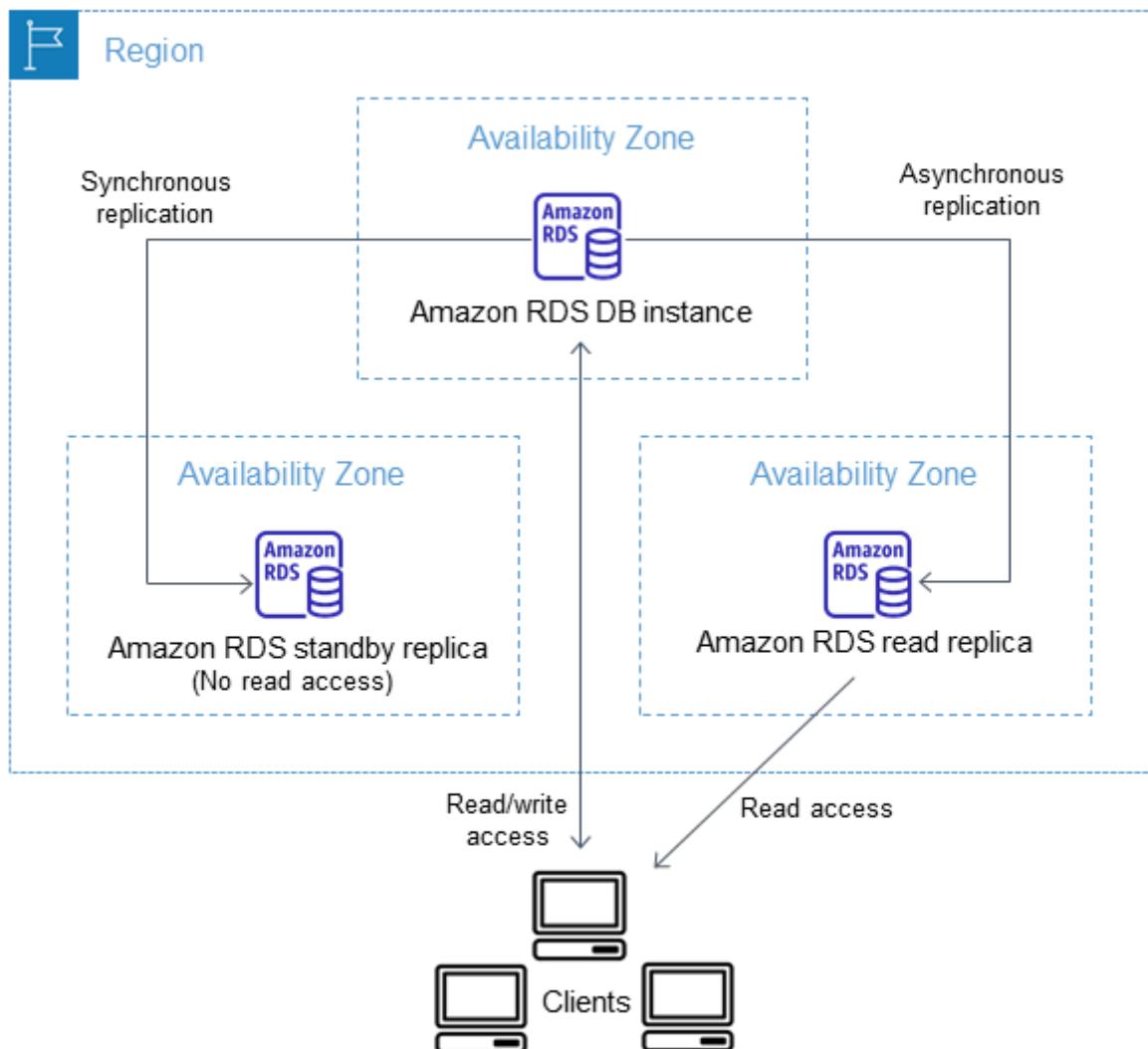
read-only connections. Applications connect to a read replica the same way they do to any DB instance. Amazon RDS replicates all databases from the source DB instance.

Note

The Oracle DB engine supports replica databases in mounted mode. A mounted replica doesn't accept user connections and so can't serve a read-only workload. The primary use for mounted replicas is cross-Region disaster recovery. For more information, see [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#).

In some cases, a read replica resides in a different AWS Region from its primary DB instance. In these cases, Amazon RDS sets up a secure communications channel between the primary DB instance and the read replica. Amazon RDS establishes any AWS security configurations needed to enable the secure channel, such as adding security group entries. For more information about cross-Region read replicas, see [Creating a read replica in a different AWS Region \(p. 383\)](#).

You can configure a read replica for a DB instance that also has a standby replica configured for high availability in a Multi-AZ deployment. Replication with the standby replica is synchronous, and the standby replica can't serve read traffic.



For more information about high availability and standby replicas, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Read replicas are supported by the MariaDB, Microsoft SQL Server, MySQL, Oracle, and PostgreSQL DB engines. In this section, you can find general information about using read replicas with all of these engines.

Topics

- [Overview of Amazon RDS read replicas \(p. 372\)](#)
- [Creating a read replica \(p. 375\)](#)
- [Promoting a read replica to be a standalone DB instance \(p. 377\)](#)
- [Monitoring read replication \(p. 380\)](#)
- [Creating a read replica in a different AWS Region \(p. 383\)](#)

For information about using read replicas with a specific engine, see the following sections:

- [Working with MariaDB read replicas \(p. 1024\)](#)
- [Working with read replicas for Microsoft SQL Server in Amazon RDS \(p. 1126\)](#)
- [Working with MySQL read replicas \(p. 1389\)](#)
- [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#)
- [Working with read replicas for Amazon RDS for PostgreSQL \(p. 1852\)](#)

Overview of Amazon RDS read replicas

Deploying one or more read replicas for a given source DB instance might make sense in a variety of scenarios, including the following:

- Scaling beyond the compute or I/O capacity of a single DB instance for read-heavy database workloads. You can direct this excess read traffic to one or more read replicas.
- Serving read traffic while the source DB instance is unavailable. In some cases, your source DB instance might not be able to take I/O requests, for example due to I/O suspension for backups or scheduled maintenance. In these cases, you can direct read traffic to your read replicas. For this use case, keep in mind that the data on the read replica might be "stale" because the source DB instance is unavailable.
- Business reporting or data warehousing scenarios where you might want business reporting queries to run against a read replica, rather than your production DB instance.
- Implementing disaster recovery. You can promote a read replica to a standalone instance as a disaster recovery solution if the primary DB instance fails.

By default, a read replica is created with the same storage type as the source DB instance. However, you can create a read replica that has a different storage type from the source DB instance based on the options listed in the following table.

Source DB instance storage type	Source DB instance storage allocation	Read replica storage type options
Provisioned IOPS	100 GiB–64 TiB	Provisioned IOPS, General Purpose, Magnetic
General Purpose	100 GiB–64 TiB	Provisioned IOPS, General Purpose, Magnetic
General Purpose	<100 GiB	General Purpose, Magnetic
Magnetic	100 GiB–6 TiB	Provisioned IOPS, General Purpose, Magnetic

Source DB instance storage type	Source DB instance storage allocation	Read replica storage type options
Magnetic	<100 GiB	General Purpose, Magnetic

Note

When you increase the allocated storage of a read replica, it must be by at least 10 percent. If you try to increase the value by less than 10 percent, you get an error.

Amazon RDS doesn't support circular replication. You can't configure a DB instance to serve as a replication source for an existing DB instance. You can only create a new read replica from an existing DB instance. For example, if **MyDBInstance** replicates to **ReadReplica1**, you can't configure **ReadReplica1** to replicate back to **MyDBInstance**. For MariaDB and MySQL, and for certain versions of PostgreSQL, you can create a read replica from an existing read replica. For example, from **ReadReplica1**, you can create a new read replica, such as **ReadReplica2**. For Oracle and SQL Server, you can't create a read replica from an existing read replica.

If you no longer need read replicas, you can explicitly delete them using the same mechanisms for deleting a DB instance. If you delete a source DB instance without deleting its read replicas in the same AWS Region, each read replica is promoted to a standalone DB instance. For information about deleting a DB instance, see [Deleting a DB instance \(p. 421\)](#). For information about read replica promotion, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

If you have cross-Region read replicas, see [Cross-Region replication considerations \(p. 387\)](#) for information related to deleting the source DB instance for a cross-Region read replica.

Differences between read replicas for different DB engines

Because Amazon RDS DB engines implement replication differently, there are several significant differences you should know about, as shown in the following table.

Feature or behavior	MySQL and MariaDB	Oracle	PostgreSQL	SQL Server
What is the replication method?	Logical replication.	Physical replication.	Physical replication.	Physical replication.
How are transaction logs purged?	RDS for MySQL and RDS for MariaDB keep any binary logs that haven't been applied.	If a primary DB instance has no cross-Region read replicas, Amazon RDS for Oracle keeps a minimum of two hours of transaction logs on the source DB instance. Logs are purged from the source DB instance after two hours or after the archive log retention hours setting has passed, whichever is longer. Logs are purged from the read replica	PostgreSQL has the parameter <code>wal_keep_segments</code> that dictates how many write ahead log (WAL) files are kept to provide data to the read replicas. The parameter value specifies the number of logs to keep.	The Virtual Log File (VLF) of the transaction log file on the primary replica can be truncated after it is no longer required for the secondary replicas. The VLF can only be marked as inactive

Feature or behavior	MySQL and MariaDB	Oracle	PostgreSQL	SQL Server
		<p>after the archive log retention hours setting has passed only if they have been successfully applied to the database.</p> <p>In some cases, a primary DB instance might have one or more cross-Region read replicas. If so, Amazon RDS for Oracle keeps the transaction logs on the source DB instance until they have been transmitted and applied to all cross-Region read replicas.</p> <p>For information about setting archive log retention hours, see Retaining archived redo logs (p. 1564).</p>		when the log records have been hardened in the replicas. Regardless of how fast the disk subsystems are in the primary replica, the transaction log will keep the VLFs until the slowest replica has hardened it.
Can a replica be made writable?	Yes. You can enable the MySQL or MariaDB read replica to be writable.	No. An Oracle read replica is a physical copy, and Oracle doesn't allow for writes in a read replica. You can promote the read replica to make it writable. The promoted read replica has the replicated data to the point when the request was made to promote it.	No. A PostgreSQL read replica is a physical copy, and PostgreSQL doesn't allow for a read replica to be made writable.	No. A SQL Server read replica is a physical copy and also doesn't allow for writes. You can promote the read replica to make it writable. The promoted read replica has the replicated data up to the point when the request was made to promote it.

Feature or behavior	MySQL and MariaDB	Oracle	PostgreSQL	SQL Server
Can backups be performed on the replica?	Yes. Automatic backups and manual snapshots are supported on RDS for MySQL or RDS for MariaDB read replicas.	Yes. Automatic backups and manual snapshots are supported on RDS for Oracle read replicas.	Yes, you can create a manual snapshot of RDS for PostgreSQL read replicas, but automatic backups aren't supported.	No. Automatic backups and manual snapshots aren't supported on RDS for SQL Server read replicas.
Can you use parallel replication?	Yes. All supported MariaDB and MySQL versions allow for parallel replication threads.	Yes. Redo log data is always transmitted in parallel from the primary database to all of its read replicas.	No. PostgreSQL has a single process handling replication.	Yes. Redo log data is always transmitted in parallel from the primary database to all of its read replicas.
Can you maintain a replica in a mounted rather than a read-only state?	No.	Yes. The primary use for mounted replicas is cross-Region disaster recovery. An Active Data Guard license isn't required for mounted replicas. For more information, see Working with read replicas for Amazon RDS for Oracle (p. 1630) .	No.	No.

Creating a read replica

You can create a read replica from an existing DB instance using the AWS Management Console, AWS CLI, or RDS API. You create a read replica by specifying `SourceDBInstanceIdentifier`, which is the DB instance identifier of the source DB instance that you want to replicate from.

When you create a read replica, Amazon RDS takes a DB snapshot of your source DB instance and begins replication. As a result, you experience a brief I/O suspension on your source DB instance while the DB snapshot occurs.

Note

The I/O suspension typically lasts about one minute. You can avoid the I/O suspension if the source DB instance is a Multi-AZ deployment, because in that case the snapshot is taken from the secondary DB instance.

An active, long-running transaction can slow the process of creating the read replica. We recommend that you wait for long-running transactions to complete before creating a read replica. If you create multiple read replicas in parallel from the same source DB instance, Amazon RDS takes only one snapshot at the start of the first create action.

When creating a read replica, there are a few things to consider. First, you must enable automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica. To enable automatic backups on an RDS for MySQL read replica, first create the read replica, then modify the read replica to enable automatic backups.

Note

Within an AWS Region, we strongly recommend that you create all read replicas in the same virtual private cloud (VPC) based on Amazon VPC as the source DB instance. If you create a read replica in a different VPC from the source DB instance, classless inter-domain routing (CIDR) ranges can overlap between the replica and the RDS system. CIDR overlap makes the replica unstable, which can negatively impact applications connecting to it. If you receive an error when creating the read replica, choose a different destination DB subnet group. For more information, see [Working with a DB instance in a VPC \(p. 2103\)](#).

You can't create a read replica in a different AWS account from the source DB instance.

Console

To create a read replica from a source DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to use as the source for a read replica.
4. For **Actions**, choose **Create read replica**.
5. For **DB instance identifier**, enter a name for the read replica.
6. Choose your instance specifications. We recommend that you use the same DB instance class and storage type as the source DB instance for the read replica.
7. For **Multi-AZ deployment**, choose **Yes** to create a standby of your replica in another Availability Zone for failover support for the replica.

Note

Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

8. To create an encrypted read replica:
 - a. Choose **Enable encryption**.
 - b. For **AWS KMS key**, choose the AWS KMS key identifier of the KMS key.

Note

The source DB instance must be encrypted. To learn more about encrypting the source DB instance, see [Encrypting Amazon RDS resources \(p. 2000\)](#).

9. Specify other settings, such as storage autoscaling.

For information about each setting, see [Settings for DB instances \(p. 237\)](#).

10. Choose **Create read replica**.

After the read replica is created, you can see it on the **Databases** page in the RDS console. It shows **Replica** in the **Role** column.

AWS CLI

To create a read replica from a source DB instance, use the AWS CLI command `create-db-instance-read-replica`. This example also enables storage autoscaling.

You can specify other settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance-read-replica \
--db-instance-identifier myreadreplica \
--source-db-instance-identifier mydbinstance \
--max-allocated-storage 1000
```

For Windows:

```
aws rds create-db-instance-read-replica ^
--db-instance-identifier myreadreplica ^
--source-db-instance-identifier mydbinstance ^
--max-allocated-storage 1000
```

RDS API

To create a read replica from a source MySQL, MariaDB, Oracle, PostgreSQL, or SQL Server DB instance, call the Amazon RDS API [CreateDBInstanceReadReplica](#) operation with the following required parameters:

- `DBInstanceIdentifier`
- `SourceDBInstanceIdentifier`

Promoting a read replica to be a standalone DB instance

You can promote a read replica into a standalone DB instance. When you promote a read replica, the DB instance is rebooted before it becomes available.



There are several reasons you might want to promote a read replica to a standalone DB instance:

- **Performing DDL operations (MySQL and MariaDB only)** – DDL operations, such as creating or rebuilding indexes, can take time and impose a significant performance penalty on your DB instance. You can perform these operations on a MySQL or MariaDB read replica once the read replica is in sync with its primary DB instance. Then you can promote the read replica and direct your applications to use the promoted instance.
- **Sharding** – Sharding embodies the "share-nothing" architecture and essentially involves breaking a large database into several smaller databases. One common way to split a database is splitting tables that are not joined in the same query onto different hosts. Another method is duplicating a table across multiple hosts and then using a hashing algorithm to determine which host receives a given update. You can create read replicas corresponding to each of your shards (smaller databases) and

promote them when you decide to convert them into standalone shards. You can then carve out the key space (if you are splitting rows) or distribution of tables for each of the shards depending on your requirements.

- **Implementing failure recovery** – You can use read replica promotion as a data recovery scheme if the primary DB instance fails. This approach complements synchronous replication, automatic failure detection, and failover.

If you are aware of the ramifications and limitations of asynchronous replication and you still want to use read replica promotion for data recovery, you can. To do this, first create a read replica and then monitor the primary DB instance for failures. In the event of a failure, do the following:

1. Promote the read replica.
2. Direct database traffic to the promoted DB instance.
3. Create a replacement read replica with the promoted DB instance as its source.

When you promote a read replica, the new DB instance that is created retains the option group and the parameter group of the former read replica. The promotion process can take several minutes or longer to complete, depending on the size of the read replica. After you promote the read replica to a new DB instance, it's just like any other DB instance. For example, you can create read replicas from the new DB instance and perform point-in-time restore operations. Because the promoted DB instance is no longer a read replica, you can't use it as a replication target. If a source DB instance has several read replicas, promoting one of the read replicas to a DB instance has no effect on the other replicas.

Backup duration is a function of the number of changes to the database since the previous backup. If you plan to promote a read replica to a standalone instance, we recommend that you enable backups and complete at least one backup prior to promotion. In addition, you can't promote a read replica to a standalone instance when it has the backing-up status. If you have enabled backups on your read replica, configure the automated backup window so that daily backups don't interfere with read replica promotion.

The following steps show the general process for promoting a read replica to a DB instance:

1. Stop any transactions from being written to the primary DB instance, and then wait for all updates to be made to the read replica. Database updates occur on the read replica after they have occurred on the primary DB instance, and this replication lag can vary significantly. Use the [Replica Lag](#) metric to determine when all updates have been made to the read replica.
2. For MySQL and MariaDB only: If you need to make changes to the MySQL or MariaDB read replica, you must set the `read_only` parameter to `0` in the DB parameter group for the read replica. You can then perform all needed DDL operations, such as creating indexes, on the read replica. Actions taken on the read replica don't affect the performance of the primary DB instance.
3. Promote the read replica by using the **Promote** option on the Amazon RDS console, the AWS CLI command [promote-read-replica](#), or the [PromoteReadReplica](#) Amazon RDS API operation.

Note

The promotion process takes a few minutes to complete. When you promote a read replica, replication is stopped and the read replica is rebooted. When the reboot is complete, the read replica is available as a new DB instance.

4. (Optional) Modify the new DB instance to be a Multi-AZ deployment. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#) and [Multi-AZ deployments for high availability \(p. 121\)](#).

Console

To promote a read replica to a standalone DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the Amazon RDS console, choose **Databases**.
The **Databases** pane appears. Each read replica shows **Replica** in the **Role** column.
3. Choose the read replica that you want to promote.
4. For **Actions**, choose **Promote**.
5. On the **Promote Read Replica** page, enter the backup retention period and the backup window for the newly promoted DB instance.
6. When the settings are as you want them, choose **Continue**.
7. On the acknowledgment page, choose **Promote Read Replica**.

AWS CLI

To promote a read replica to a standalone DB instance, use the AWS CLI `promote-read-replica` command.

Example

For Linux, macOS, or Unix:

```
aws rds promote-read-replica \
--db-instance-identifier myreadreplica
```

For Windows:

```
aws rds promote-read-replica ^
--db-instance-identifier myreadreplica
```

RDS API

To promote a read replica to a standalone DB instance, call the Amazon RDS API `PromoteReadReplica` operation with the required parameter `DBInstanceIdentifier`.

Monitoring read replication

You can monitor the status of a read replica in several ways. The Amazon RDS console shows the status of a read replica in the **Replication** section of the **Connectivity & security** tab in the read replica details. To view the details for a read replica, choose the name of the read replica in the list of DB instances in the Amazon RDS console.

Replication (2)			
<input type="text"/> Filter by replication			
DB instance	Role	Region & AZ	Replication source
mydbinstancecf	Primary	us-east-1d	-
mydbinstancecfreplica	Replica	us-east-1f	mydbinstancecf

You can also see the status of a read replica using the AWS CLI `describe-db-instances` command or the Amazon RDS API `DescribeDBInstances` operation.

The status of a read replica can be one of the following:

- **replicating** – The read replica is replicating successfully.
- **replication degraded (SQL Server only)** – Replicas are receiving data from the primary instance, but one or more databases might be not getting updates. This can occur, for example, when a replica is in the process of setting up newly created databases.

The status doesn't transition from `replication degraded` to `error`, unless an error occurs during the degraded state.

- **error** – An error has occurred with the replication. Check the **Replication Error** field in the Amazon RDS console or the event log to determine the exact error. For more information about troubleshooting a replication error, see [Troubleshooting a MySQL read replica problem \(p. 1399\)](#).
- **terminated (MariaDB, MySQL, or PostgreSQL only)** – Replication is terminated. This occurs if replication is stopped for more than 30 consecutive days, either manually or due to a replication error. In this case, Amazon RDS terminates replication between the primary DB instance and all read replicas. Amazon RDS does this to prevent increased storage requirements on the source DB instance and long failover times.

Broken replication can affect storage because the logs can grow in size and number due to the high volume of errors messages being written to the log. Broken replication can also affect failure recovery due to the time Amazon RDS requires to maintain and process the large number of logs during recovery.

- **terminated (Oracle only)** – Replication is terminated. This occurs if replication is stopped for more than 8 hours because there isn't enough storage remaining on the read replica. In this case, Amazon RDS terminates replication between the primary DB instance and the affected read replica. This status is a terminal state, and the read replica must be re-created.
- **stopped (MariaDB or MySQL only)** – Replication has stopped because of a customer-initiated request.
- **replication stop point set (MySQL only)** – A customer-initiated stop point was set using the [`mysql.rds_start_replication_until` \(p. 1452\)](#) stored procedure and the replication is in progress.
- **replication stop point reached (MySQL only)** – A customer-initiated stop point was set using the [`mysql.rds_start_replication_until` \(p. 1452\)](#) stored procedure and replication is stopped because the stop point was reached.

You can see where a DB instance is being replicated and if so, check its replication status. On the **Databases** page in the RDS console, it shows **Primary** in the **Role** column. Choose its DB instance name. On its detail page, on the **Connectivity & security** tab, its replication status is under **Replication**.

Monitoring replication lag

You can monitor replication lag in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric.

For MariaDB and MySQL, the ReplicaLag metric reports the value of the Seconds_Behind_Master field of the SHOW REPLICA STATUS command. Common causes for replication lag for MySQL and MariaDB are the following:

- A network outage.
- Writing to tables with indexes on a read replica. If the `read_only` parameter is not set to 0 on the read replica, it can break replication.
- Using a nontransactional storage engine such as MyISAM. Replication is only supported for the InnoDB storage engine on MySQL and the XtraDB storage engine on MariaDB.

Note

Previous versions of MariaDB and MySQL used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MariaDB version before 10.5 or a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

When the ReplicaLag metric reaches 0, the replica has caught up to the primary DB instance. If the ReplicaLag metric returns -1, then replication is currently not active. ReplicaLag = -1 is equivalent to Seconds_Behind_Master = NULL.

For Oracle, the ReplicaLag metric is the sum of the Apply Lag value and the difference between the current time and the apply lag's DATUM_TIME value. The DATUM_TIME value is the last time the read replica received data from its source DB instance. For more information, see [V\\$DATAGUARD_STATS](#) in the Oracle documentation.

For SQL Server, the ReplicaLag metric is the maximum lag of databases that have fallen behind, in seconds. For example, if you have two databases that lag 5 seconds and 10 seconds, respectively, then ReplicaLag is 10 seconds. The ReplicaLag metric returns the value of the following query.

```
SELECT MAX(secondary_lag_seconds) max_lag FROM sys.dm_hadr_database_replica_states;
```

For more information, see [secondary_lag_seconds](#) in the Microsoft documentation.

ReplicaLag returns -1 if RDS can't determine the lag, such as during replica setup, or when the read replica is in the `error` state.

Note

New databases aren't included in the lag calculation until they are accessible on the read replica.

For PostgreSQL, the ReplicaLag metric returns the value of the following query.

```
SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS reader_lag
```

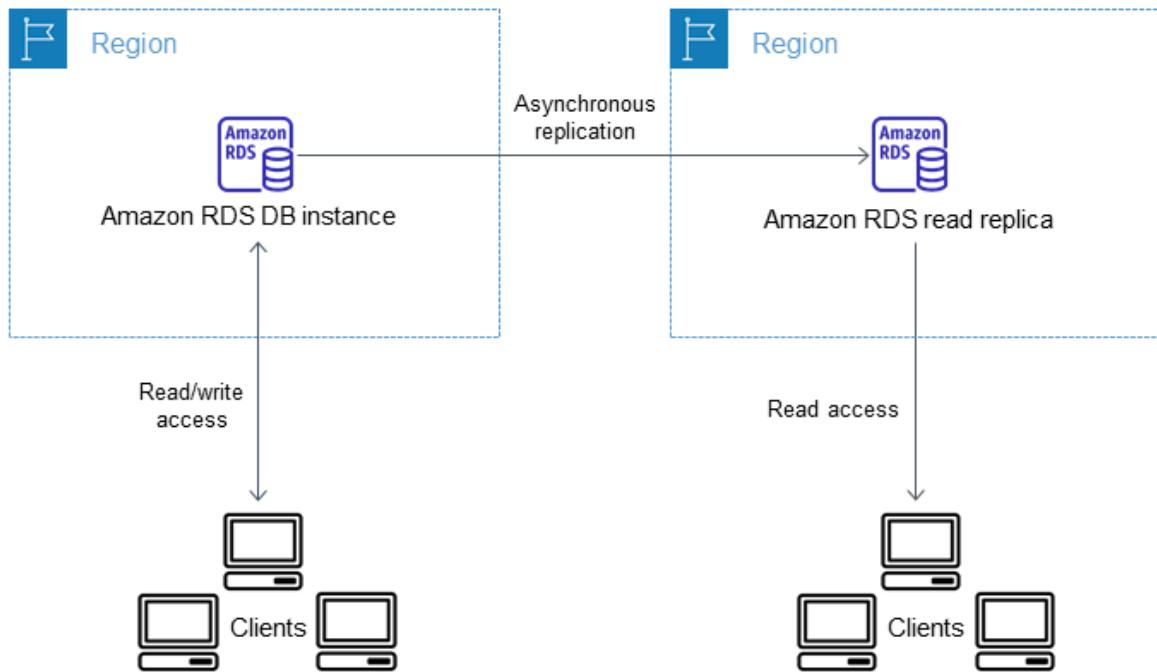
PostgreSQL versions 9.5.2 and later use physical replication slots to manage write ahead log (WAL) retention on the source instance. For each cross-Region read replica instance, Amazon RDS creates a physical replication slot and associates it with the instance. Two Amazon CloudWatch metrics, Oldest

Replication Slot Lag and Transaction Logs Disk Usage, show how far behind the most lagging replica is in terms of WAL data received and how much storage is being used for WAL data. The Transaction Logs Disk Usage value can substantially increase when a cross-Region read replica is lagging significantly.

For more information about monitoring a DB instance with CloudWatch, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).

Creating a read replica in a different AWS Region

With Amazon RDS, you can create a read replica in a different AWS Region from the source DB instance.



You create a read replica in a different AWS Region to do the following:

- Improve your disaster recovery capabilities.
- Scale read operations into an AWS Region closer to your users.
- Make it easier to migrate from a data center in one AWS Region to a data center in another AWS Region.

Creating a read replica in a different AWS Region from the source instance is similar to creating a replica in the same AWS Region. You can use the AWS Management Console, run the [create-db-instance-read-replica](#) command, or call the [CreateDBInstanceReadReplica](#) API operation.

Note

To create an encrypted read replica in a different AWS Region from the source DB instance, the source DB instance must be encrypted.

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability with cross-Region replication, see [Cross-Region read replicas \(p. 83\)](#).

Creating a cross-Region read replica

The following procedures show how to create a read replica from a source MariaDB, Microsoft SQL Server, MySQL, Oracle, or PostgreSQL DB instance in a different AWS Region.

Console

You can create a read replica across AWS Regions using the AWS Management Console.

To create a read replica across AWS Regions with the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the MariaDB, Microsoft SQL Server, MySQL, Oracle, or PostgreSQL DB instance that you want to use as the source for a read replica.
4. For **Actions**, choose **Create read replica**.
5. For **DB instance identifier**, enter a name for the read replica.
6. Choose the **Destination Region**.
7. Choose the instance specifications you want to use. We recommend that you use the same DB instance class and storage type for the read replica.
8. To create an encrypted read replica in another AWS Region:
 - a. Choose **Enable encryption**.
 - b. For **AWS KMS key**, choose the AWS KMS key identifier of the KMS key in the destination AWS Region.

Note

To create an encrypted read replica, the source DB instance must be encrypted. To learn more about encrypting the source DB instance, see [Encrypting Amazon RDS resources \(p. 2000\)](#).

9. Choose other options, such as storage autoscaling.
10. Choose **Create read replica**.

AWS CLI

To create a read replica from a source MySQL, Microsoft SQL Server, MariaDB, Oracle, or PostgreSQL DB instance in a different AWS Region, you can use the `create-db-instance-read-replica` command. In this case, you use `create-db-instance-read-replica` from the AWS Region where you want the read replica (destination Region) and specify the Amazon Resource Name (ARN) for the source DB instance. An ARN uniquely identifies a resource created in Amazon Web Services.

For example, if your source DB instance is in the US East (N. Virginia) Region, the ARN looks similar to this example:

```
arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

For information about ARNs, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

To create a read replica in a different AWS Region from the source DB instance, you can use the AWS CLI `create-db-instance-read-replica` command from the destination AWS Region. The following parameters are required for creating a read replica in another AWS Region:

- **--region** – The destination AWS Region where the read replica is created.
- **--source-db-instance-identifier** – The DB instance identifier for the source DB instance. This identifier must be in the ARN format for the source AWS Region.
- **--db-instance-identifier** – The identifier for the read replica in the destination AWS Region.

Example of a cross-Region read replica

The following code creates a read replica in the US West (Oregon) Region from a source DB instance in the US East (N. Virginia) Region.

For Linux, macOS, or Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

For Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --region us-west-2 ^
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

The following parameter is also required for creating an encrypted read replica in another AWS Region:

- **--kms-key-id** – The AWS KMS key identifier of the KMS key to use to encrypt the read replica in the destination AWS Region.

Example of an encrypted cross-Region read replica

The following code creates an encrypted read replica in the US West (Oregon) Region from a source DB instance in the US East (N. Virginia) Region.

For Linux, macOS, or Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance \
    --kms-key-id my-us-west-2-key
```

For Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --region us-west-2 ^
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance ^
    --kms-key-id my-us-west-2-key
```

The **--source-region** option is required when you're creating an encrypted read replica between the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. For **--source-region**, specify the AWS Region of the source DB instance.

If `--source-region` isn't specified, specify a `--pre-signed-url` value. A *presigned URL* is a URL that contains a Signature Version 4 signed request for the `create-db-instance-read-replica` command that's called in the source AWS Region. To learn more about the `pre-signed-url` option, see [create-db-instance-read-replica](#) in the *AWS CLI Command Reference*.

RDS API

To create a read replica from a source MySQL, Microsoft SQL Server, MariaDB, Oracle, or PostgreSQL DB instance in a different AWS Region, you can call the Amazon RDS API operation [CreateDBInstanceReadReplica](#). In this case, you call [CreateDBInstanceReadReplica](#) from the AWS Region where you want the read replica (destination Region) and specify the Amazon Resource Name (ARN) for the source DB instance. An ARN uniquely identifies a resource created in Amazon Web Services.

To create an encrypted read replica in a different AWS Region from the source DB instance, you can use the Amazon RDS API [CreateDBInstanceReadReplica](#) operation from the destination AWS Region. To create an encrypted read replica in another AWS Region, you must specify a value for `PreSignedURL`. `PreSignedURL` should contain a request for the [CreateDBInstanceReadReplica](#) operation to call in the source AWS Region where the read replica is created in. To learn more about `PreSignedUrl`, see [CreateDBInstanceReadReplica](#).

For example, if your source DB instance is in the US East (N. Virginia) Region, the ARN looks similar to the following.

```
arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

For information about ARNs, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

Example

```
https://us-west-2.rds.amazonaws.com/
?Action=CreateDBInstanceReadReplica
&KmsKeyId=my-us-east-1-key
&PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F
%253FAction%253DCreateDBInstanceReadReplica
%2526DestinationRegion%253Dus-east-1
%2526KmsKeyId%253Dmy-us-east-1-key
%2526SourceDBInstanceIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-
west-2%123456789012%25253Adb%25253Amydbinstance
%2526SignatureMethod%253DHmacSHA256
%2526SignatureVersion%253D4%2526SourceDBInstanceIdentifier%253Darn%25253Aaws
%25253Ards%25253Aus-west-2%25253A123456789012%25253Ainstance%25253Amydbinstance
%2526Version%253D2014-10-31
%2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256
%2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-west-2%252Frds
%252Faws4_request
%2526X-Amz-Date%253D20161117T215409Z
%2526X-Amz-Expires%253D3600
%2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-amz-
content-sha256%253Bx-amz-date
%2526X-Amz-Signature
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613
&DBInstanceIdentifier=myreadreplica
&SourceDBInstanceIdentifier=&region-arn;rds:us-east-1:123456789012:db:mydbinstance
&Version=2012-01-15
&SignatureVersion=2
&SignatureMethod=HmacSHA256
&Timestamp=2012-01-20T22%3A06%3A23.624Z
&AWSAccessKeyId=<&AWS; Access Key ID>
&Signature=<Signature>
```

How Amazon RDS does cross-Region replication

Amazon RDS uses the following process to create a cross-Region read replica. Depending on the AWS Regions involved and the amount of data in the databases, this process can take hours to complete. You can use this information to determine how far the process has proceeded when you create a cross-Region read replica:

1. Amazon RDS begins configuring the source DB instance as a replication source and sets the status to *modifying*.
2. Amazon RDS begins setting up the specified read replica in the destination AWS Region and sets the status to *creating*.
3. Amazon RDS creates an automated DB snapshot of the source DB instance in the source AWS Region. The format of the DB snapshot name is `rds:<InstanceID>-<timestamp>`, where `<InstanceID>` is the identifier of the source instance, and `<timestamp>` is the date and time the copy started. For example, `rds:mysourceinstance-2013-11-14-09-24` was created from the instance `mysourceinstance` at `2013-11-14-09-24`. During the creation of an automated DB snapshot, the source DB instance status remains *modifying*, the read replica status remains *creating*, and the DB snapshot status is *creating*. The progress column of the DB snapshot page in the console reports how far the DB snapshot creation has progressed. When the DB snapshot is complete, the status of both the DB snapshot and source DB instance are set to *available*.
4. Amazon RDS begins a cross-Region snapshot copy for the initial data transfer. The snapshot copy is listed as an automated snapshot in the destination AWS Region with a status of *creating*. It has the same name as the source DB snapshot. The progress column of the DB snapshot display indicates how far the copy has progressed. When the copy is complete, the status of the DB snapshot copy is set to *available*.
5. Amazon RDS then uses the copied DB snapshot for the initial data load on the read replica. During this phase, the read replica is in the list of DB instances in the destination, with a status of *creating*. When the load is complete, the read replica status is set to *available*, and the DB snapshot copy is deleted.
6. When the read replica reaches the available status, Amazon RDS starts by replicating the changes made to the source instance since the start of the create read replica operation. During this phase, the replication lag time for the read replica is greater than 0.

For information about replication lag time, see [Monitoring read replication \(p. 380\)](#).

Cross-Region replication considerations

All of the considerations for performing replication within an AWS Region apply to cross-Region replication. The following extra considerations apply when replicating between AWS Regions:

- A source DB instance can have cross-Region read replicas in multiple AWS Regions.
- You can replicate between the GovCloud (US-East) and GovCloud (US-West) Regions, but not into or out of GovCloud (US).
- For Microsoft SQL Server, Oracle, and PostgreSQL DB instances, you can only create a cross-Region Amazon RDS read replica from a source Amazon RDS DB instance that is not a read replica of another Amazon RDS DB instance. This limitation doesn't apply to MariaDB and MySQL DB instances.
- You can expect to see a higher level of lag time for any read replica that is in a different AWS Region than the source instance. This lag time comes from the longer network channels between regional data centers.
- For cross-Region read replicas, any of the create read replica commands that specify the `--db-subnet-group-name` parameter must specify a DB subnet group from the same VPC.
- Due to the limit on the number of access control list (ACL) entries for a VPC, we can't guarantee more than five cross-Region read replica instances.

- In most cases, the read replica uses the default DB parameter group and DB option group for the specified DB engine.

For the MySQL and Oracle DB engines, you can specify a custom parameter group for the read replica in the `--db-parameter-group-name` option of the AWS CLI command [create-db-instance-read-replica](#). You can't specify a custom parameter group when you use the AWS Management Console.

- The read replica uses the default security group.
- For MariaDB, Microsoft SQL Server, MySQL, and Oracle DB instances, when the source DB instance for a cross-Region read replica is deleted, the read replica is promoted.
- For PostgreSQL DB instances, when the source DB instance for a cross-Region read replica is deleted, the replication status of the read replica is set to terminated. The read replica isn't promoted.

You have to promote the read replica manually or delete it.

Requesting a cross-Region read replica

To communicate with the source Region to request the creation of a cross-Region read replica, the requester (IAM role or IAM user) must have access to the source DB instance and the source Region.

Certain conditions in the requester's IAM policy can cause the request to fail. The following examples assume that the source DB instance is in US East (Ohio) and the read replica is created in US East (N. Virginia). These examples show conditions in the requester's IAM policy that cause the request to fail:

- The requester's policy has a condition for `aws:RequestedRegion`.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": "us-east-1"
    }
}
```

The request fails because the policy doesn't allow access to the source Region. For a successful request, specify both the source and destination Regions.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2"
        ]
    }
}
```

- The requester's policy doesn't allow access to the source DB instance.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "arn:aws:rds:us-east-1:123456789012:db:myreadreplica"
```

...

For a successful request, specify both the source instance and the replica.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": [
    "arn:aws:rds:us-east-1:123456789012:db:myreadreplica",
    "arn:aws:rds:us-east-2:123456789012:db:mydbinstance"
]
...
```

- The requester's policy denies aws:ViaAWSservice.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "Bool": {"aws:ViaAWSservice": "false"}
}
```

Communication with the source Region is made by RDS on the requester's behalf. For a successful request, don't deny calls made by AWS services.

- The requester's policy has a condition for aws:SourceVpc or aws:SourceVpce.

These requests might fail because when RDS makes the call to the remote Region, it isn't from the specified VPC or VPC endpoint.

If you need to use one of the previous conditions that would cause a request to fail, you can include a second statement with aws:CalledVia in your policy to make the request succeed. For example, you can use aws:CalledVia with aws:SourceVpce as shown here:

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:SourceVpce": "vpce-1a2b3c4d"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "rds:CreateDBInstanceReadReplica"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "rds.amazonaws.com"
            ]
        }
    }
}
```

For more information, see [Policies and permissions in IAM](#) in the *IAM User Guide*.

Authorizing the read replica

After a cross-Region DB read replica creation request returns success, RDS starts the replica creation in the background. An authorization for RDS to access the source DB instance is created. This authorization links the source DB instance to the read replica, and allows RDS to copy only to the specified read replica.

The authorization is verified by RDS using the `rds:CrossRegionCommunication` permission in the service-linked IAM role. If the replica is authorized, RDS communicates with the source Region and completes the replica creation.

RDS doesn't have access to DB instances that weren't authorized previously by a `CreateDBInstanceReadReplica` request. The authorization is revoked when read replica creation completes.

RDS uses the service-linked role to verify the authorization in the source Region. If you delete the service-linked role during the replication creation process, the creation fails.

For more information, see [Using service-linked roles](#) in the *IAM User Guide*.

Using AWS Security Token Service credentials

Session tokens from the global AWS Security Token Service (AWS STS) endpoint are valid only in AWS Regions that are enabled by default (commercial Regions). If you use credentials from the `assumeRole` API operation in AWS STS, use the regional endpoint if the source Region is an opt-in Region. Otherwise, the request fails. This happens because your credentials must be valid in both Regions, which is true for opt-in Regions only when the regional AWS STS endpoint is used.

To use the global endpoint, make sure that it's enabled for both Regions in the operations. Set the global endpoint to `Valid in all AWS Regions` in the AWS STS account settings.

The same rule applies to credentials in the `presigned URL` parameter.

For more information, see [Managing AWS STS in an AWS Region](#) in the *IAM User Guide*.

Cross-Region replication costs

The data transferred for cross-Region replication incurs Amazon RDS data transfer charges. These cross-Region replication actions generate charges for the data transferred out of the source AWS Region:

- When you create a read replica, Amazon RDS takes a snapshot of the source instance and transfers the snapshot to the read replica AWS Region.
- For each data modification made in the source databases, Amazon RDS transfers data from the source AWS Region to the read replica AWS Region.

For more information about data transfer pricing, see [Amazon RDS pricing](#).

For MySQL and MariaDB instances, you can reduce your data transfer costs by reducing the number of cross-Region read replicas that you create. For example, suppose that you have a source DB instance in one AWS Region and want to have three read replicas in another AWS Region. In this case, you create only one of the read replicas from the source DB instance. You create the other two replicas from the first read replica instead of the source DB instance.

For example, if you have `source-instance-1` in one AWS Region, you can do the following:

- Create `read-replica-1` in the new AWS Region, specifying `source-instance-1` as the source.
- Create `read-replica-2` from `read-replica-1`.

- Create `read-replica-3` from `read-replica-1`.

In this example, you are only charged for the data transferred from `source-instance-1` to `read-replica-1`. You aren't charged for the data transferred from `read-replica-1` to the other two replicas because they are all in the same AWS Region. If you create all three replicas directly from `source-instance-1`, you are charged for the data transfers to all three replicas.

Tagging Amazon RDS resources

You can use Amazon RDS tags to add metadata to your Amazon RDS resources. You can use the tags to add your own notations about database instances, snapshots, Aurora clusters, and so on. Doing so can help you to document your Amazon RDS resources. You can also use the tags with automated maintenance procedures.

In particular, you can use these tags with IAM policies. You can use them to manage access to RDS resources and to control what actions can be applied to the RDS resources. You can also use these tags to track costs by grouping expenses for similarly tagged resources.

You can tag the following Amazon RDS resources:

- DB instances
- DB clusters
- Read replicas
- DB snapshots
- DB cluster snapshots
- Reserved DB instances
- Event subscriptions
- DB option groups
- DB parameter groups
- DB cluster parameter groups
- DB subnet groups
- RDS Proxies
- RDS Proxy endpoints

Note

Currently, you can't tag RDS Proxies and RDS Proxy endpoints by using the AWS Management Console.

Topics

- [Overview of Amazon RDS resource tags \(p. 392\)](#)
- [Using tags for access control with IAM \(p. 393\)](#)
- [Using tags to produce detailed billing reports \(p. 393\)](#)
- [Adding, listing, and removing tags \(p. 394\)](#)
- [Using the AWS Tag Editor \(p. 396\)](#)
- [Copying tags to DB instance snapshots \(p. 396\)](#)
- [Tutorial: Use tags to specify which DB instances to stop \(p. 397\)](#)
- [Using tags to enable backups in AWS Backup \(p. 399\)](#)

Overview of Amazon RDS resource tags

An Amazon RDS tag is a name-value pair that you define and associate with an Amazon RDS resource. The name is referred to as the key. Supplying a value for the key is optional. You can use tags to assign arbitrary information to an Amazon RDS resource. You can use a tag key, for example, to define a category, and the tag value might be an item in that category. For example, you might define a tag

key of "project" and a tag value of "Salix". In this case, these indicate that the Amazon RDS resource is assigned to the Salix project. You can also use tags to designate Amazon RDS resources as being used for test or production by using a key such as environment=test or environment=production. We recommend that you use a consistent set of tag keys to make it easier to track metadata associated with Amazon RDS resources.

In addition, you can use conditions in your IAM policies to control access to AWS resources based on the tags on that resource. You can do this by using the global `aws:ResourceTag/tag-key` condition key. For more information, see [Controlling access to AWS resources](#) in the *AWS Identity and Access Management User Guide*.

Each Amazon RDS resource has a tag set, which contains all the tags that are assigned to that Amazon RDS resource. A tag set can contain as many as 50 tags, or it can be empty. If you add a tag to an RDS resource with the same key as an existing resource tag, the new value overwrites the old.

AWS doesn't apply any semantic meaning to your tags; tags are interpreted strictly as character strings. RDS can set tags on a DB instance or other RDS resources. Tag setting depends on the options that you use when you create the resource. For example, Amazon RDS might add a tag indicating that a DB instance is for production or for testing.

- The tag key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with aws:. The string can contain only the set of Unicode letters, digits, white space, '_', ':', '.', '/', '=', '+', '-', '@' (Java regex: "^(\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*\$").
 - The tag value is an optional string value of the tag. The string value can be from 1 to 256 Unicode characters in length and cannot be prefixed with aws:. The string can contain only the set of Unicode letters, digits, white space, '_', ':', '.', '/', '=', '+', '-', '@' (Java regex: "^(\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*\$").

Values do not have to be unique in a tag set and can be null. For example, you can have a key-value pair in a tag set of `project=Trinity` and `cost-center=Trinity`.

You can use the AWS Management Console, the AWS CLI, or the Amazon RDS API to add, list, and delete tags on Amazon RDS resources. When using the CLI or API, make sure to provide the Amazon Resource Name (ARN) for the RDS resource to work with. For more information about constructing an ARN, see [Constructing an ARN for Amazon RDS \(p. 402\)](#).

Tags are cached for authorization purposes. Because of this, additions and updates to tags on Amazon RDS resources can take several minutes before they are available.

Using tags for access control with IAM

You can use tags with IAM policies to manage access to Amazon RDS resources. You can also use tags to control what actions can be applied to the Amazon RDS resources.

For information on managing access to tagged resources with IAM policies, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

Using tags to produce detailed billing reports

You can also use tags to track costs by grouping expenses for similarly tagged resources.

Use tags to organize your AWS bill to reflect your own cost structure. To do this, sign up to get your AWS account bill with tag key values included. Then, to see the cost of combined resources, organize your

billing information according to resources with the same tag key values. For example, you can tag several resources with a specific application name, and then organize your billing information to see the total cost of that application across several services. For more information, see [Using Cost Allocation Tags](#) in the [AWS Billing User Guide](#).

Note

You can add a tag to a snapshot, however, your bill will not reflect this grouping.

Adding, listing, and removing tags

The following procedures show how to perform typical tagging operations on resources related to DB instances.

Console

The process to tag an Amazon RDS resource is similar for all resources. The following procedure shows how to tag an Amazon RDS DB instance.

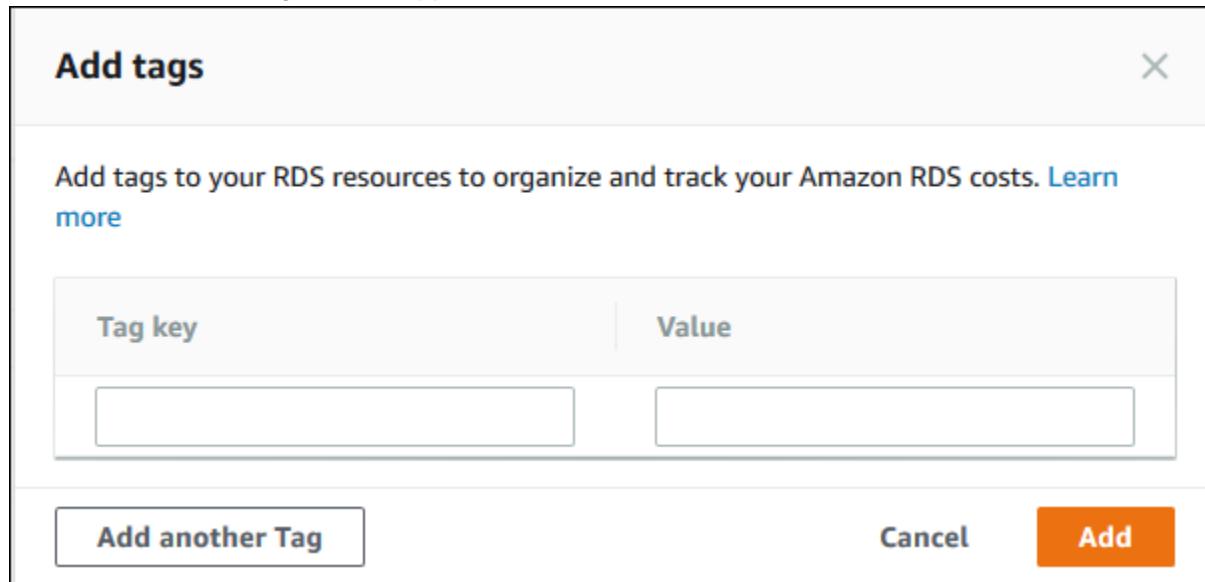
To add a tag to a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

Note

To filter the list of DB instances in the **Databases** pane, enter a text string for **Filter databases**. Only DB instances that contain the string appear.

3. Choose the name of the DB instance that you want to tag to show its details.
4. In the details section, scroll down to the **Tags** section.
5. Choose **Add**. The **Add tags** window appears.



6. Enter a value for **Tag key** and **Value**.
7. To add another tag, you can choose **Add another Tag** and enter a value for its **Tag key** and **Value**.
Repeat this step as many times as necessary.
8. Choose **Add**.

To delete a tag from a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

Note

To filter the list of DB instances in the **Databases** pane, enter a text string in the **Filter databases** box. Only DB instances that contain the string appear.

3. Choose the name of the DB instance to show its details.
4. In the details section, scroll down to the **Tags** section.
5. Choose the tag you want to delete.

Tags (1)		Edit	Delete	Add
<input type="text"/> Filter tag key		< 1 >	<input type="checkbox"/>	<input type="radio"/>
Tag key	Value			
<input checked="" type="checkbox"/> workload-type	other			

6. Choose **Delete**, and then choose **Delete** in the **Delete tags** window.

AWS CLI

You can add, list, or remove tags for a DB instance using the AWS CLI.

- To add one or more tags to an Amazon RDS resource, use the AWS CLI command [add-tags-to-resource](#).
- To list the tags on an Amazon RDS resource, use the AWS CLI command [list-tags-for-resource](#).
- To remove one or more tags from an Amazon RDS resource, use the AWS CLI command [remove-tags-from-resource](#).

To learn more about how to construct the required ARN, see [Constructing an ARN for Amazon RDS \(p. 402\)](#).

RDS API

You can add, list, or remove tags for a DB instance using the Amazon RDS API.

- To add a tag to an Amazon RDS resource, use the [AddTagsToResource](#) operation.
- To list tags that are assigned to an Amazon RDS resource, use the [ListTagsForResource](#).
- To remove tags from an Amazon RDS resource, use the [RemoveTagsFromResource](#) operation.

To learn more about how to construct the required ARN, see [Constructing an ARN for Amazon RDS \(p. 402\)](#).

When working with XML using the Amazon RDS API, tags use the following schema:

```
<Tagging>
  <TagSet>
```

```

<Tag>
  <Key>Project</Key>
  <Value>Trinity</Value>
</Tag>
<Tag>
  <Key>User</Key>
  <Value>Jones</Value>
</Tag>
</TagSet>
</Tagging>

```

The following table provides a list of the allowed XML tags and their characteristics. Values for Key and Value are case-dependent. For example, project=Trinity and PROJECT=Trinity are two distinct tags.

Tagging element	Description
TagSet	A tag set is a container for all tags assigned to an Amazon RDS resource. There can be only one tag set per resource. You work with a TagSet only through the Amazon RDS API.
Tag	A tag is a user-defined key-value pair. There can be from 1 to 50 tags in a tag set.
Key	A key is the required name of the tag. The string value can be from 1 to 128 Unicode characters in length and cannot be prefixed with aws: or rds:. The string can only contain only the set of Unicode letters, digits, white space, '_', '.', '/', '=', '+', '-' (Java regex: " <code>^([\u00p{L}\u00p{Z}\u00p{N}_:=+\u00p{-}]*\$</code> "). Keys must be unique to a tag set. For example, you cannot have a key-pair in a tag set with the key the same but with different values, such as project/Trinity and project/Xanadu.
Value	A value is the optional value of the tag. The string value can be from 1 to 256 Unicode characters in length and cannot be prefixed with aws: or rds:. The string can only contain only the set of Unicode letters, digits, white space, '_', '.', '/', '=', '+', '-' (Java regex: " <code>^([\u00p{L}\u00p{Z}\u00p{N}_:=+\u00p{-}]*\$</code> "). Values do not have to be unique in a tag set and can be null. For example, you can have a key-value pair in a tag set of project/Trinity and cost-center/Trinity.

Using the AWS Tag Editor

You can browse and edit the tags on your RDS resources in the AWS Management Console by using the AWS Tag editor. For more information, see [Tag Editor](#) in the *AWS Resource Groups User Guide*.

Copying tags to DB instance snapshots

When you create or restore a DB instance, you can specify that the tags from the DB instance are copied to snapshots of the DB instance. Copying tags ensures that the metadata for the DB snapshots matches that of the source DB instance. It also ensures that any access policies for the DB snapshots also match those of the source DB instance.

You can specify that tags are copied to DB snapshots for the following actions:

- Creating a DB instance.

- Restoring a DB instance.
- Creating a read replica.
- Copying a DB snapshot.

In most cases, tags aren't copied by default. However, when you restore a DB instance from a DB snapshot, RDS checks whether you specify new tags. If yes, the new tags are added to the restored DB instance. If there are no new tags, RDS looks for the tags from the source DB instance for the DB snapshot. RDS then adds those tags to the restored DB instance.

To prevent tags from source DB instances from being added to restored DB instances, we recommend that you specify new tags when restoring a DB instance.

Note

In some cases, you might include a value for the `--tag-key` parameter of the `create-db-snapshot` AWS CLI command. Or you might supply at least one tag to the `CreateDBSnapshot` API operation. In these cases, RDS doesn't copy tags from the source DB instance to the new DB snapshot. This functionality applies even if the source DB instance has the `--copy-tags-to-snapshot` (`CopyTagsToSnapshot`) option turned on.

If you take this approach, you can create a copy of a DB instance from a DB snapshot. This approach avoids adding tags that don't apply to the new DB instance. You create your DB snapshot using the AWS CLI `create-db-snapshot` command (or the `CreateDBSnapshot` RDS API operation). After you create your DB snapshot, you can add tags as described later in this topic.

Tutorial: Use tags to specify which DB instances to stop

Suppose that you're creating a number of DB instances in a development or test environment. You need to keep all of these DB instances for several days. Some of the DB instances run tests overnight. Other DB instances can be stopped overnight and started again the next day. The following example shows how to assign a tag to those DB instances that are suitable to stop overnight. Then the example shows how a script can detect which DB instances have that tag and then stop those DB instances. In this example, the value portion of the key-value pair doesn't matter. The presence of the `stopable` tag signifies that the DB instance has this user-defined property.

To specify which DB instances to stop

1. Determine the ARN of a DB instance that you want to designate as stoppable.

The commands and APIs for tagging work with ARNs. That way, they can work seamlessly across AWS Regions, AWS accounts, and different types of resources that might have identical short names. You can specify the ARN instead of the DB instance ID in CLI commands that operate on DB instances. Substitute the name of your own DB instances for `dev-test-db-instance`. In subsequent commands that use ARN parameters, substitute the ARN of your own DB instance. The ARN includes your own AWS account ID and the name of the AWS Region where your DB instance is located.

```
$ aws rds describe-db-instances --db-instance-identifier dev-test-db-instance \
  --query "*[].{DBInstance:DBInstanceArn}" --output text
arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
```

2. Add the tag `stopable` to this DB instance.

You choose the name for this tag. This approach means that you can avoid devising a naming convention that encodes all relevant information in names. In such a convention, you might encode information in the DB instance name or names of other resources. Because this example treats

the tag as an attribute that is either present or absent, it omits the Value= part of the --tags parameter.

```
$ aws rds add-tags-to-resource \
--resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance \
--tags Key=stoppable
```

3. Confirm that the tag is present in the DB instance.

These commands retrieve the tag information for the DB instance in JSON format and in plain tab-separated text.

```
$ aws rds list-tags-for-resource \
--resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
{
    "TagList": [
        {
            "Key": "stoppable",
            "Value": ""
        }
    ]
}
aws rds list-tags-for-resource \
--resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance --output
text
TAGLIST stoppable
```

4. To stop all the DB instances that are designated as stoppable, prepare a list of all your DB instances. Loop through the list and check if each DB instance is tagged with the relevant attribute.

This Linux example uses shell scripting. This scripting saves the list of DB instance ARNs to a temporary file and then performs CLI commands for each DB instance.

```
$ aws rds describe-db-instances --query "[].[DBInstanceArn]" --output text >/tmp/
db_instance_arns.lst
$ for arn in $(cat /tmp/db_instance_arns.lst)
do
    match=$(aws rds list-tags-for-resource --resource-name $arn --output text | grep
stoppable)"
    if [[ ! -z "$match" ]]
    then
        echo "DB instance $arn is tagged as stoppable. Stopping it now."
    # Note that you need to get the DB instance identifier from the ARN.
        dbid=$(echo $arn | sed -e 's/.*/\1')
        aws rds stop-db-instance --db-instance-identifier $dbid
    fi
done

DB instance arn:arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance is tagged as
stoppable. Stopping it now.
{
    "DBInstance": {
        "DBInstanceIdentifier": "dev-test-db-instance",
        "DBInstanceClass": "db.t3.medium",
        ...
    }
}
```

You can run a script like this at the end of each day to make sure that nonessential DB instances are stopped. You might also schedule a job using a utility such as cron to perform such a check each night. For example, you might do this in case some DB instances were left running by mistake. Here, you might fine-tune the command that prepares the list of DB instances to check.

The following command produces a list of your DB instances, but only the ones in available state. The script can ignore DB instances that are already stopped, because they will have different status values such as stopped or stopping.

```
$ aws rds describe-db-instances \
--query '[].{DBInstanceArn:DBInstanceArn,DBInstanceStatus:DBInstanceState}|?DBInstanceState == `available`|[]|.{DBInstanceArn:DBInstanceArn}' \
--output text
arn:aws:rds:us-east-1:123456789102:db:db-instance-2447
arn:aws:rds:us-east-1:123456789102:db:db-instance-3395
arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
arn:aws:rds:us-east-1:123456789102:db:pg2-db-instance
```

Tip

You can use assigning tags and finding DB instances with those tags to reduce costs in other ways. For example, take this scenario with DB instances used for development and testing. In this case, you might designate some DB instances to be deleted at the end of each day. Or you might designate them to have their DB instances changed to small DB instance classes during times of expected low usage.

Using tags to enable backups in AWS Backup

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises. You can manage backups of your Amazon RDS DB instances in AWS Backup.

To enable backups in AWS Backup, you use resource tagging to associate your DB instance with a backup plan.

This example assumes that you have already created a backup plan in AWS Backup. You use exactly the same tag for your DB instance that is in your backup plan, as shown in the following figure.

Backup plan tags (1)		Edit	Delete	Add
<input type="text"/> Filter by tags				« 1 » @
<input type="checkbox"/>	Tag key		Value	
<input type="checkbox"/>	BackupPlan		Test	

For more information about AWS Backup, see the [AWS Backup Developer Guide](#).

You can assign a tag to a DB instance using the AWS Management Console, the AWS CLI, or the RDS API. The following examples are for the console and CLI.

Console

To assign a tag to a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the link for the DB instance to which you want to assign a tag.
4. On the database details page, choose the **Tags** tab.
5. Under **Tags**, choose **Add tags**.
6. Under **Add tags**:

- a. For **Tag key**, enter **BackupPlan**.
- b. For **Value**, enter **Test**.
- c. Choose **Add**.

The result is shown under **Tags**.

Tags (1)	
<input type="checkbox"/>	Tags
<input type="checkbox"/>	BackupPlan
	Value
	Test

CLI

To assign a tag to a DB instance

- Use the following CLI command:

For Linux, macOS, or Unix:

```
aws rds add-tags-to-resource \
--resource-name arn:aws:rds:us-east-1:123456789012:db:new-orcl-db \
--tags Key=BackupPlan,Value=Test
```

For Windows:

```
aws rds add-tags-to-resource ^
--resource-name arn:aws:rds:us-east-1:123456789012:db:new-orcl-db ^
--tags Key=BackupPlan,Value=Test
```

The `add-tags-to-resource` CLI command returns no output.

To confirm that the DB instance is tagged

- Use the following CLI command:

For Linux, macOS, or Unix:

```
aws rds list-tags-for-resource \
--resource-name arn:aws:rds:us-east-1:123456789012:db:new-orcl-db
```

For Windows:

```
aws rds list-tags-for-resource ^
--resource-name arn:aws:rds:us-east-1:123456789012:db:new-orcl-db
```

The `list-tags-for-resource` CLI command returns the following output:

```
{
  "TagList": [
    {
      "Key": "BackupPlan",
      "Value": "Test"
    }
  ]
}
```

Working with Amazon Resource Names (ARNs) in Amazon RDS

Resources created in Amazon Web Services are each uniquely identified with an Amazon Resource Name (ARN). For certain Amazon RDS operations, you must uniquely identify an Amazon RDS resource by specifying its ARN. For example, when you create an RDS DB instance read replica, you must supply the ARN for the source DB instance.

Constructing an ARN for Amazon RDS

Resources created in Amazon Web Services are each uniquely identified with an Amazon Resource Name (ARN). You can construct an ARN for an Amazon RDS resource using the following syntax.

`arn:aws:rds:<region>:<account number>:<resourcetype>:<name>`

Region Name	Region	Endpoint	Protocol	
US East (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS	
		rds-fips.us-east-2.api.aws	HTTPS	
		rds.us-east-2.api.aws	HTTPS	
		rds-fips.us-east-2.amazonaws.com	HTTPS	
US East (N. Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS	
		rds-fips.us-east-1.api.aws	HTTPS	
		rds-fips.us-east-1.amazonaws.com	HTTPS	
		rds.us-east-1.api.aws	HTTPS	
US West (N. California)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS	
		rds.us-west-1.api.aws	HTTPS	
		rds-fips.us-west-1.amazonaws.com	HTTPS	
		rds-fips.us-west-1.api.aws	HTTPS	
US West (Oregon)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS	
		rds-fips.us-west-2.amazonaws.com	HTTPS	
		rds.us-west-2.api.aws	HTTPS	
		rds-fips.us-west-2.api.aws	HTTPS	
Africa (Cape Town)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS	
		rds.af-south-1.api.aws	HTTPS	
Asia Pacific	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS	
		rds.ap-east-1.api.aws	HTTPS	

Region Name	Region	Endpoint	Protocol	
(Hong Kong)				
Asia Pacific (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS	
Asia Pacific (Jakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com	HTTPS	
Asia Pacific (Mumbai)	ap-south-1	rds.ap-south-1.amazonaws.com rds.ap-south-1.api.aws	HTTPS HTTPS	
Asia Pacific (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com rds.ap-northeast-3.api.aws	HTTPS HTTPS	
Asia Pacific (Seoul)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com rds.ap-northeast-2.api.aws	HTTPS HTTPS	
Asia Pacific (Singapore)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com rds.ap-southeast-1.api.aws	HTTPS HTTPS	
Asia Pacific (Sydney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com rds.ap-southeast-2.api.aws	HTTPS HTTPS	
Asia Pacific (Tokyo)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com rds.ap-northeast-1.api.aws	HTTPS HTTPS	
Canada (Central)	ca-central-1	rds.ca-central-1.amazonaws.com rds.ca-central-1.api.aws rds-fips.ca-central-1.api.aws rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS HTTPS HTTPS	
Europe (Frankfurt)	eu-central-1	rds.eu-central-1.amazonaws.com rds.eu-central-1.api.aws	HTTPS HTTPS	
Europe (Ireland)	eu-west-1	rds.eu-west-1.amazonaws.com rds.eu-west-1.api.aws	HTTPS HTTPS	
Europe (London)	eu-west-2	rds.eu-west-2.amazonaws.com rds.eu-west-2.api.aws	HTTPS HTTPS	
Europe (Milan)	eu-south-1	rds.eu-south-1.amazonaws.com rds.eu-south-1.api.aws	HTTPS HTTPS	

Region Name	Region	Endpoint	Protocol	
Europe (Paris)	eu-west-3	rds.eu-west-3.amazonaws.com rds.eu-west-3.api.aws	HTTPS HTTPS	
Europe (Spain)	eu-south-2	rds.eu-south-2.amazonaws.com	HTTPS	
Europe (Stockholm)	eu-north-1	rds.eu-north-1.amazonaws.com rds.eu-north-1.api.aws	HTTPS HTTPS	
Europe (Zurich)	eu-central-2	rds.eu-central-2.amazonaws.com	HTTPS	
Middle East (Bahrain)	me-south-1	rds.me-south-1.amazonaws.com rds.me-south-1.api.aws	HTTPS HTTPS	
Middle East (UAE)	me-central-1	rds.me-central-1.amazonaws.com	HTTPS	
South America (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com rds.sa-east-1.api.aws	HTTPS HTTPS	
AWS GovCloud (US-East)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (US-West)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com	HTTPS	

The following table shows the format that you should use when constructing an ARN for a particular Amazon RDS resource type.

Resource type	ARN format
DB instance	<p>arn:aws:rds:<region>:<account>:db:<name></p> <p>For example:</p> <pre>arn:aws:rds:us-east-2:123456789012:db:my-mysql-instance-1</pre>
DB cluster	<p>arn:aws:rds:<region>:<account>:cluster:<name></p> <p>For example:</p> <pre>arn:aws:rds:us-east-2:123456789012:cluster:my-aurora-cluster-1</pre>
Event subscription	arn:aws:rds:<region>:<account>:es:<name>

Resource type	ARN format
	For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:es:my-subscription </div>
DB option group	arn:aws:rds:<region>:<account>:og:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:og:my-og </div>
DB parameter group	arn:aws:rds:<region>:<account>:pg:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:pg:my-param-enable-logs </div>
DB cluster parameter group	arn:aws:rds:<region>:<account>:cluster-pg:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:cluster-pg:my-cluster-param-timezone </div>
Reserved DB instance	arn:aws:rds:<region>:<account>:ri:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:ri:my-reserved-postgresql </div>
DB security group	arn:aws:rds:<region>:<account>:secgrp:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:secgrp:my-public </div>
Automated DB snapshot	arn:aws:rds:<region>:<account>:snapshot:rds:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:snapshot:rds:my-mysql-db-2019-07-22-07-23 </div>
Automated DB cluster snapshot	arn:aws:rds:<region>:<account>:cluster-snapshot:rds:<name> For example: <div style="border: 1px solid black; padding: 5px; background-color: #f9f9f9;"> arn:aws:rds:us-east-2:123456789012:cluster-snapshot:rds:my-aurora-cluster-2019-07-22-16-16 </div>

Resource type	ARN format
Manual DB snapshot	<p>arn:aws:rds:<region>:<account>:snapshot:<name></p> <p>For example:</p> <pre>arn:aws:rds:us-east-2:123456789012:snapshot:my-mysql-db-snap</pre>
Manual DB cluster snapshot	<p>arn:aws:rds:<region>:<account>:cluster-snapshot:<name></p> <p>For example:</p> <pre>arn:aws:rds:us-east-2:123456789012:cluster-snapshot:my-aurora-cluster-snap</pre>
DB subnet group	<p>arn:aws:rds:<region>:<account>:subgrp:<name></p> <p>For example:</p> <pre>arn:aws:rds:us-east-2:123456789012:subgrp:my-subnet-10</pre>

Getting an existing ARN

You can get the ARN of an RDS resource by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or RDS API.

Console

To get an ARN from the AWS Management Console, navigate to the resource you want an ARN for, and view the details for that resource. For example, you can get the ARN for a DB instance from the **Configuration** tab of the DB instance details, as shown following.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below it, the 'Instance' section is expanded, showing various configuration details. The 'ARN' field, which contains the value 'arn:aws:rds:us-west-2:XXXXXXXXXX:db:oracle-instance1', is highlighted with a large red oval.

DB instance id	oracle-instance1
Engine version	12.1.0.2.v14
Storage type	General Purpose (SSD)
IOPS	-
Storage	20 GiB
DB name	ORCL
License model	Bring Your Own License
Character set	AL32UTF8
Option groups	default:oracle-ee-12-1
ARN	arn:aws:rds:us-west-2:XXXXXXXXXX:db:oracle-instance1
Resource id	XXXXXXXXXX

AWS CLI

To get an ARN from the AWS CLI for a particular RDS resource, you use the `describe` command for that resource. The following table shows each AWS CLI command, and the ARN property used with the command to get an ARN.

AWS CLI command	ARN property
<code>describe-event-subscriptions</code>	<code>EventSubscriptionArn</code>
<code>describe-certificates</code>	<code>CertificateArn</code>

AWS CLI command	ARN property
describe-db-parameter-groups	DBParameterGroupArn
describe-db-cluster-parameter-groups	DBClusterParameterGroupArn
describe-db-instances	DBInstanceArn
describe-db-security-groups	DBSecurityGroupArn
describe-db-snapshots	DBSnapshotArn
describe-events	SourceArn
describe-reserved-db-instances	ReservedDBInstanceArn
describe-db-subnet-groups	DBSubnetGroupArn
describe-option-groups	OptionGroupArn
describe-db-clusters	DBClusterArn
describe-db-cluster-snapshots	DBClusterSnapshotArn

For example, the following AWS CLI command gets the ARN for a DB instance.

Example

For Linux, macOS, or Unix:

```
aws rds describe-db-instances \
--db-instance-identifier DBInstanceIdentifier \
--region us-west-2 \
--query "*[].[DBInstanceIdentifier,DBInstanceArn,DBInstanceArn]"
```

For Windows:

```
aws rds describe-db-instances ^
--db-instance-identifier DBInstanceIdentifier ^
--region us-west-2 ^
--query "*[].[DBInstanceIdentifier,DBInstanceArn,DBInstanceArn]"
```

The output of that command is like the following:

```
[  
  {  
    "DBInstanceArn": "arn:aws:rds:us-west-2:account_id:db:instance_id",  
    "DBInstanceIdentifier": "instance_id"  
  }  
]
```

RDS API

To get an ARN for a particular RDS resource, you can call the following RDS API operations and use the ARN properties shown following.

RDS API operation	ARN property
DescribeEventSubscriptions	EventSubscriptionArn
DescribeCertificates	CertificateArn
DescribeDBParameterGroups	DBParameterGroupArn
DescribeDBClusterParameterGroups	DBClusterParameterGroupArn
DescribeDBInstances	DBInstanceArn
DescribeDBSecurityGroups	DBSecurityGroupArn
DescribeDBSchemas	DBSnapshotArn
DescribeEvents	SourceArn
DescribeReservedDBInstances	ReservedDBInstanceArn
DescribeDBSubnetGroups	DBSubnetGroupArn
DescribeOptionGroups	OptionGroupArn
DescribeDBClusters	DBClusterArn
DescribeDBClusterSnapshots	DBClusterSnapshotArn

Working with storage for Amazon RDS DB instances

To specify how you want your data stored in Amazon RDS, choose a storage type and provide a storage size when you create or modify a DB instance. Later, you can increase the amount or change the type of storage by modifying the DB instance. For more information about which storage type to use for your workload, see [Amazon RDS storage types \(p. 64\)](#).

Topics

- [Increasing DB instance storage capacity \(p. 410\)](#)
- [Managing capacity automatically with Amazon RDS storage autoscaling \(p. 412\)](#)
- [Modifying settings for Provisioned IOPS SSD storage \(p. 416\)](#)
- [I/O-intensive storage modifications \(p. 418\)](#)
- [Modifying settings for General Purpose SSD \(gp3\) storage \(p. 418\)](#)

Increasing DB instance storage capacity

If you need space for additional data, you can scale up the storage of an existing DB instance. To do so, you can use the Amazon RDS Management Console, the Amazon RDS API, or the AWS Command Line Interface (AWS CLI). For information about storage limits, see [Amazon RDS DB instance storage \(p. 64\)](#).

Note

Scaling storage for Amazon RDS for Microsoft SQL Server DB instances is supported only for General Purpose SSD or Provisioned IOPS SSD storage types.

To monitor the amount of free storage for your DB instance so you can respond when necessary, we recommend that you create an Amazon CloudWatch alarm. For more information on setting CloudWatch alarms, see [Using CloudWatch alarms](#).

Scaling storage usually doesn't cause any outage or performance degradation of the DB instance. After you modify the storage size for a DB instance, the status of the DB instance is **storage-optimization**.

Note

Storage optimization can take several hours. You can't make further storage modifications for either six (6) hours or until storage optimization has completed on the instance, whichever is longer.

However, a special case is if you have a SQL Server DB instance and haven't modified the storage configuration since November 2017. In this case, you might experience a short outage of a few minutes when you modify your DB instance to increase the allocated storage. After the outage, the DB instance is online but in the **storage-optimization** state. Performance might be degraded during storage optimization.

Note

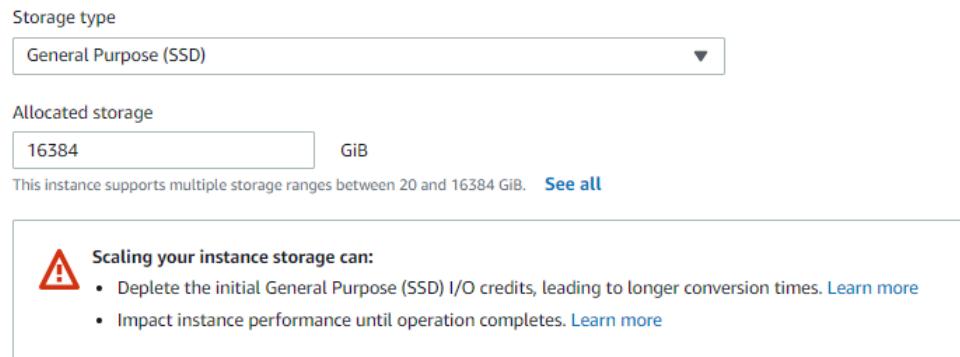
You can't reduce the amount of storage for a DB instance after storage has been allocated. When you increase the allocated storage, it must be by at least 10 percent. If you try to increase the value by less than 10 percent, you get an error.

Console

To increase storage for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify.
4. Choose **Modify**.
5. Enter a new value for **Allocated storage**. It must be greater than the current value.



6. Choose **Continue** to move to the next screen.
7. Choose **Apply immediately** in the **Scheduling of modifications** section to apply the storage changes to the DB instance immediately.
Or choose **Apply during the next scheduled maintenance window** to apply the changes during the next maintenance window.
8. When the settings are as you want them, choose **Modify DB instance**.

AWS CLI

To increase the storage for a DB instance, use the AWS CLI command `modify-db-instance`. Set the following parameters:

- `--allocated-storage` – Amount of storage to be allocated for the DB instance, in gibibytes.
- `--apply-immediately` – Use `--apply-immediately` to apply the storage changes immediately.
Or use `--no-apply-immediately` (the default) to apply the changes during the next maintenance window. An immediate outage occurs when the changes are applied.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

RDS API

To increase storage for a DB instance, use the Amazon RDS API operation `ModifyDBInstance`. Set the following parameters:

- `AllocatedStorage` – Amount of storage to be allocated for the DB instance, in gibibytes.
- `ApplyImmediately` – Set this option to `True` to apply the storage changes immediately. Set this option to `False` (the default) to apply the changes during the next maintenance window. An immediate outage occurs when the changes are applied.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

Managing capacity automatically with Amazon RDS storage autoscaling

If your workload is unpredictable, you can enable storage autoscaling for an Amazon RDS DB instance. To do so, you can use the Amazon RDS console, the Amazon RDS API, or the AWS CLI.

For example, you might use this feature for a new mobile gaming application that users are adopting rapidly. In this case, a rapidly increasing workload might exceed the available database storage. To avoid having to manually scale up database storage, you can use Amazon RDS storage autoscaling.

With storage autoscaling enabled, when Amazon RDS detects that you are running out of free database space it automatically scales up your storage. Amazon RDS starts a storage modification for an autoscaling-enabled DB instance when these factors apply:

- Free available space is less than 10 percent of the allocated storage.
- The low-storage condition lasts at least five minutes.
- At least six hours have passed since the last storage modification, or storage optimization has completed on the instance, whichever is longer.

The additional storage is in increments of whichever of the following is greater:

- 5 GiB
- 10 percent of currently allocated storage
- Storage growth prediction for 7 hours based on the `FreeStorageSpace` metrics change in the past hour. For more information on metrics, see [Monitoring with Amazon CloudWatch](#).

The maximum storage threshold is the limit that you set for autoscaling the DB instance. It has the following constraints:

- You must set the maximum storage threshold to at least 10% more than the current allocated storage. We recommend setting it to at least 26% more to avoid receiving an [event notification \(p. 674\)](#) that the storage size is approaching the maximum storage threshold.

For example, if you have DB instance with 1000 GiB of allocated storage, then set the maximum storage threshold to at least 1100 GiB. If you don't, you get an error such as Invalid max storage size for `engine_name`. However, we recommend that you set the maximum storage threshold to at least 1260 GiB to avoid the event notification.

- For a DB instance that uses Provisioned IOPS storage, the ratio of IOPS to maximum storage threshold (in GiB) must be from 1–50 on RDS for SQL Server, and 0.5–50 on other RDS DB engines.
- You can't set the maximum storage threshold for autoscaling-enabled instances to a value greater than the maximum allocated storage for the database engine and DB instance class.

For example, SQL Server Standard Edition on db.m5.xlarge has a default allocated storage for the instance of 20 GiB (the minimum) and a maximum allocated storage of 16,384 GiB. The default maximum storage threshold for autoscaling is 1,000 GiB. If you use this default, the instance doesn't autoscale above 1,000 GiB. This is true even though the maximum allocated storage for the instance is 16,384 GiB.

Note

We recommend that you carefully choose the maximum storage threshold based on usage patterns and customer needs. If there are any aberrations in the usage patterns, the maximum storage threshold can prevent scaling storage to an unexpectedly high value when autoscaling

predicts a very high threshold. After a DB instance has been autoscaled, its allocated storage can't be reduced.

Topics

- [Limitations \(p. 413\)](#)
- [Enabling storage autoscaling for a new DB instance \(p. 413\)](#)
- [Changing the storage autoscaling settings for a DB instance \(p. 414\)](#)
- [Turning off storage autoscaling for a DB instance \(p. 415\)](#)

Limitations

The following limitations apply to storage autoscaling:

- Autoscaling doesn't occur if the maximum storage threshold would be equaled or exceeded by the storage increment.
- When autoscaling, RDS predicts the storage size for subsequent autoscaling operations. If a subsequent operation is predicted to exceed the maximum storage threshold, then RDS autoscales to the maximum storage threshold.
- Autoscaling can't completely prevent storage-full situations for large data loads. This is because further storage modifications can't be made for either six (6) hours or until storage optimization has completed on the instance, whichever is longer.

If you perform a large data load, and autoscaling doesn't provide enough space, the database might remain in the storage-full state for several hours. This can harm the database.

- If you start a storage scaling operation at the same time that Amazon RDS starts an autoscaling operation, your storage modification takes precedence. The autoscaling operation is canceled.
- Autoscaling can't be used with magnetic storage.
- Autoscaling can't be used with the following previous-generation instance classes that have less than 6 TiB of orderable storage: db.m3.large, db.m3.xlarge, and db.m3.2xlarge.
- Autoscaling operations aren't logged by AWS CloudTrail. For more information on CloudTrail, see [Monitoring Amazon RDS API calls in AWS CloudTrail \(p. 725\)](#).

Although automatic scaling helps you to increase storage on your Amazon RDS DB instance dynamically, you should still configure the initial storage for your DB instance to an appropriate size for your typical workload.

Enabling storage autoscaling for a new DB instance

When you create a new Amazon RDS DB instance, you can choose whether to enable storage autoscaling. You can also set an upper limit on the storage that Amazon RDS can allocate for the DB instance.

Note

When you clone an Amazon RDS DB instance that has storage autoscaling enabled, that setting isn't automatically inherited by the cloned instance. The new DB instance has the same amount of allocated storage as the original instance. You can turn storage autoscaling on again for the new instance if the cloned instance continues to increase its storage requirements.

Console

To enable storage autoscaling for a new DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the upper-right corner of the Amazon RDS console, choose the AWS Region where you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**. On the **Select engine** page, choose your database engine and specify your DB instance information as described in [Getting started with Amazon RDS \(p. 153\)](#).
5. In the **Storage autoscaling** section, set the **Maximum storage threshold** value for the DB instance.
6. Specify the rest of your DB instance information as described in [Getting started with Amazon RDS \(p. 153\)](#).

AWS CLI

To enable storage autoscaling for a new DB instance, use the AWS CLI command [create-db-instance](#). Set the following parameter:

- `--max-allocated-storage` – Turns on storage autoscaling and sets the upper limit on storage size, in gibibytes.

To verify that Amazon RDS storage autoscaling is available for your DB instance, use the AWS CLI [describe-valid-db-instance-modifications](#) command. To check based on the instance class before creating an instance, use the [describe-orderable-db-instance-options](#) command. Check the following field in the return value:

- `SupportsStorageAutoscaling` – Indicates whether the DB instance or instance class supports storage autoscaling.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

RDS API

To enable storage autoscaling for a new DB instance, use the Amazon RDS API operation [CreateDBInstance](#). Set the following parameter:

- `MaxAllocatedStorage` – Turns on Amazon RDS storage autoscaling and sets the upper limit on storage size, in gibibytes.

To verify that Amazon RDS storage autoscaling is available for your DB instance, use the Amazon RDS API [DescribeValidDbInstanceModifications](#) operation for an existing instance, or the [DescribeOrderableDBInstanceOptions](#) operation before creating an instance. Check the following field in the return value:

- `SupportsStorageAutoscaling` – Indicates whether the DB instance supports storage autoscaling.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

Changing the storage autoscaling settings for a DB instance

You can turn storage autoscaling on for an existing Amazon RDS DB instance. You can also change the upper limit on the storage that Amazon RDS can allocate for the DB instance.

Console

To change the storage autoscaling settings for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify, and choose **Modify**. The **Modify DB instance** page appears.
4. Change the storage limit in the **Autoscaling** section. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
5. When all the changes are as you want them, choose **Continue** and check your modifications.
6. On the confirmation page, review your changes. If they're correct, choose **Modify DB Instance** to save your changes. If they aren't correct, choose **Back** to edit your changes or **Cancel** to cancel your changes.

Changing the storage autoscaling limit occurs immediately. This setting ignores the **Apply immediately** setting.

AWS CLI

To change the storage autoscaling settings for a DB instance, use the AWS CLI command `modify-db-instance`. Set the following parameter:

- `--max-allocated-storage` – Sets the upper limit on storage size, in gibibytes. If the value is greater than the `--allocated-storage` parameter, storage autoscaling is turned on. If the value is the same as the `--allocated-storage` parameter, storage autoscaling is turned off.

To verify that Amazon RDS storage autoscaling is available for your DB instance, use the AWS CLI `describe-valid-db-instance-modifications` command. To check based on the instance class before creating an instance, use the `describe-orderable-db-instance-options` command. Check the following field in the return value:

- `SupportsStorageAutoscaling` – Indicates whether the DB instance supports storage autoscaling.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

RDS API

To change the storage autoscaling settings for a DB instance, use the Amazon RDS API operation `ModifyDBInstance`. Set the following parameter:

- `MaxAllocatedStorage` – Sets the upper limit on storage size, in gibibytes.

To verify that Amazon RDS storage autoscaling is available for your DB instance, use the Amazon RDS API `DescribeValidDbInstanceModifications` operation for an existing instance, or the `DescribeOrderableDBInstanceOptions` operation before creating an instance. Check the following field in the return value:

- `SupportsStorageAutoscaling` – Indicates whether the DB instance supports storage autoscaling.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

Turning off storage autoscaling for a DB instance

If you no longer need Amazon RDS to automatically increase the storage for an Amazon RDS DB instance, you can turn off storage autoscaling. After you do, you can still manually increase the amount of storage for your DB instance.

Console

To turn off storage autoscaling for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify and choose **Modify**. The **Modify DB instance** page appears.
4. Clear the **Enable storage autoscaling** check box in the **Storage autoscaling** section. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
5. When all the changes are as you want them, choose **Continue** and check the modifications.
6. On the confirmation page, review your changes. If they're correct, choose **Modify DB Instance** to save your changes. If they aren't correct, choose **Back** to edit your changes or **Cancel** to cancel your changes.

Changing the storage autoscaling limit occurs immediately. This setting ignores the **Apply immediately** setting.

AWS CLI

To turn off storage autoscaling for a DB instance, use the AWS CLI command `modify-db-instance` and the following parameter:

- `--max-allocated-storage` – Specify a value equal to the `--allocated-storage` setting to prevent further Amazon RDS storage autoscaling for the specified DB instance.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

RDS API

To turn off storage autoscaling for a DB instance, use the Amazon RDS API operation `ModifyDBInstance`. Set the following parameter:

- `MaxAllocatedStorage` – Specify a value equal to the `AllocatedStorage` setting to prevent further Amazon RDS storage autoscaling for the specified DB instance.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

Modifying settings for Provisioned IOPS SSD storage

You can modify the settings for a DB instance that uses Provisioned IOPS SSD storage by using the Amazon RDS console, AWS CLI, or Amazon RDS API. Specify the storage type, allocated storage, and the amount of Provisioned IOPS that you require. The range depends on your database engine and instance type.

Although you can reduce the amount of IOPS provisioned for your instance, you can't reduce the storage size.

In most cases, scaling storage doesn't require any outage and doesn't degrade performance of the server. After you modify the storage IOPS for a DB instance, the status of the DB instance is **storage-optimization**.

Note

Storage optimization can take several hours. You can't make further storage modifications for either six (6) hours or until storage optimization has completed on the instance, whichever is longer.

For information on the ranges of allocated storage and Provisioned IOPS available for each database engine, see [Provisioned IOPS SSD storage \(p. 66\)](#).

Console

To change the Provisioned IOPS settings for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

To filter the list of DB instances, for **Filter databases** enter a text string for Amazon RDS to use to filter the results. Only DB instances whose names contain the string appear.

3. Choose the DB instance with Provisioned IOPS that you want to modify.
4. Choose **Modify**.
5. On the **Modify DB instance** page, choose **Provisioned IOPS SSD (io1)** for **Storage type**.
6. For **Provisioned IOPS**, enter a value.

If the value that you specify for either **Allocated storage** or **Provisioned IOPS** is outside the limits supported by the other parameter, a warning message is displayed. This message gives the range of values required for the other parameter.

7. Choose **Continue**.
8. Choose **Apply immediately** in the **Scheduling of modifications** section to apply the changes to the DB instance immediately. Or choose **Apply during the next scheduled maintenance window** to apply the changes during the next maintenance window.

An immediate outage occurs when the storage type changes. For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

9. Review the parameters to be changed, and choose **Modify DB instance** to complete the modification.

The new value for allocated storage or for Provisioned IOPS appears in the **Status** column.

AWS CLI

To change the Provisioned IOPS setting for a DB instance, use the AWS CLI command [modify-db-instance](#). Set the following parameters:

- **--storage-type** – Set to **io1** for Provisioned IOPS.
- **--allocated-storage** – Amount of storage to be allocated for the DB instance, in gibibytes.
- **--iops** – The new amount of Provisioned IOPS for the DB instance, expressed in I/O operations per second.
- **--apply-immediately** – Use **--apply-immediately** to apply changes immediately. Use **--no-apply-immediately** (the default) to apply changes during the next maintenance window.

RDS API

To change the Provisioned IOPS settings for a DB instance, use the Amazon RDS API operation [ModifyDBInstance](#). Set the following parameters:

- `StorageType` – Set to `io1` for Provisioned IOPS.
- `AllocatedStorage` – Amount of storage to be allocated for the DB instance, in gibibytes.
- `Iops` – The new IOPS rate for the DB instance, expressed in I/O operations per second.
- `ApplyImmediately` – Set this option to `True` to apply changes immediately. Set this option to `False` (the default) to apply changes during the next maintenance window.

I/O-intensive storage modifications

Amazon RDS DB instances use Amazon Elastic Block Store (EBS) volumes for database and log storage. Depending on the amount of storage requested, RDS (except for RDS for SQL Server) automatically *stripes* across multiple Amazon EBS volumes to enhance performance. RDS DB instances with SSD storage types are backed by either one or four striped Amazon EBS volumes in a RAID 0 configuration. By design, storage modification operations for an RDS DB instance have minimal impact on ongoing database operations.

In most cases, storage scaling modifications are completely offloaded to the Amazon EBS layer and are transparent to the database. This process is typically completed within a few minutes. However, some older RDS storage volumes require a different process for modifying the size, Provisioned IOPS, or storage type. This involves making a full copy of the data using a potentially I/O-intensive operation.

Storage modification uses an I/O-intensive operation if any of the following factors apply:

- The source storage type is magnetic. Magnetic storage doesn't support elastic volume modification.
- The RDS DB instance isn't on a one- or four-volume Amazon EBS layout. You can view the number of Amazon EBS volumes in use on your RDS DB instances by using Enhanced Monitoring metrics. For more information, see [Viewing OS metrics in the RDS console \(p. 605\)](#).
- The target size of the modification request increases the allocated storage above 400 GiB for RDS for MariaDB, MySQL, and PostgreSQL instances, and 200 GiB for RDS for Oracle. Storage autoscaling operations have the same effect when they increase the allocated storage size of your DB instance above these thresholds.

If your storage modification involves an I/O-intensive operation, it consumes I/O resources and increases the load on your DB instance. Storage modifications with I/O-intensive operations involving General Purpose SSD (gp2) storage can deplete your I/O credit balance, resulting in longer conversion times.

We recommend as a best practice to schedule these storage modification requests outside of peak hours to help reduce the time required to complete the storage modification operation. Alternatively, you can create a read replica of the DB instance and perform the storage modification on the read replica. Then promote the read replica to be the primary DB instance. For more information, see [Working with read replicas \(p. 370\)](#).

For more information, see [Why is an Amazon RDS DB instance stuck in the modifying state when I try to increase the allocated storage?](#)

Modifying settings for General Purpose SSD (gp3) storage

You can modify the settings for a DB instance that uses General Purpose SSD (gp3) storage by using the Amazon RDS console, AWS CLI, or Amazon RDS API. Specify the storage type, allocated storage, amount of Provisioned IOPS, and storage throughput that you require. Although you can reduce the amount of IOPS provisioned for your instance, you can't reduce the storage size.

In most cases, scaling storage doesn't require any outage. After you modify the storage IOPS for a DB instance, the status of the DB instance is **storage-optimization**. You can expect elevated latencies,

but still within the single-digit millisecond range, during storage optimization. The DB instance is fully operational after a storage modification.

Note

You can't make further storage modifications until six (6) hours after storage optimization has completed on the instance.

For information on the ranges of allocated storage, Provisioned IOPS, and storage throughput available for each database engine, see [gp3 storage \(p. 65\)](#).

Console

To change the storage performance settings for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

To filter the list of DB instances, for **Filter databases** enter a text string for Amazon RDS to use to filter the results. Only DB instances whose names contain the string appear.

3. Choose the DB instance with gp3 storage that you want to modify.
4. Choose **Modify**.
5. On the **Modify DB Instance page**, choose **General Purpose SSD (gp3)** for **Storage type**, then do the following:
 - a. For **Provisioned IOPS**, choose a value.
If the value that you specify for either **Allocated storage** or **Provisioned IOPS** is outside the limits supported by the other parameter, a warning message appears. This message gives the range of values required for the other parameter.
 - b. For **Storage throughput**, choose a value.
If the value that you specify for either **Provisioned IOPS** or **Storage throughput** is outside the limits supported by the other parameter, a warning message appears. This message gives the range of values required for the other parameter.
6. Choose **Continue**.
7. Choose **Apply immediately** in the **Scheduling of modifications** section to apply the changes to the DB instance immediately. Or choose **Apply during the next scheduled maintenance window** to apply the changes during the next maintenance window.
An immediate outage occurs when the storage type changes. For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).
8. Review the parameters to be changed, and choose **Modify DB instance** to complete the modification.

The new value for Provisioned IOPS appears in the **Status** column.

AWS CLI

To change the storage performance settings for a DB instance, use the AWS CLI command `modify-db-instance`. Set the following parameters:

- `--storage-type` – Set to gp3 for General Purpose SSD (gp3).
- `--allocated-storage` – Amount of storage to be allocated for the DB instance, in gibibytes.
- `--iops` – The new amount of Provisioned IOPS for the DB instance, expressed in I/O operations per second.

- **--storage-throughput** – The new storage throughput for the DB instance, expressed in MiBps.
- **--apply-immediately** – Use **--apply-immediately** to apply changes immediately. Use **--no-apply-immediately** (the default) to apply changes during the next maintenance window.

RDS API

To change the storage performance settings for a DB instance, use the Amazon RDS API operation [ModifyDBInstance](#). Set the following parameters:

- **StorageType** – Set to gp3 for General Purpose SSD (gp3).
- **AllocatedStorage** – Amount of storage to be allocated for the DB instance, in gibibytes.
- **Iops** – The new IOPS rate for the DB instance, expressed in I/O operations per second.
- **StorageThroughput** – The new storage throughput for the DB instance, expressed in MiBps.
- **ApplyImmediately** – Set this option to True to apply changes immediately. Set this option to False (the default) to apply changes during the next maintenance window.

Deleting a DB instance

To delete a DB instance, you must do the following:

- Provide the name of the instance
- Enable or disable the option to take a final DB snapshot of the instance
- Enable or disable the option to retain automated backups

If you delete a DB instance that has read replicas in the same AWS Region, each read replica is promoted to a standalone DB instance. For more information, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#). If your DB instance has read replicas in different AWS Regions, see [Cross-Region replication considerations \(p. 387\)](#) for information related to deleting the source DB instance for a cross-Region read replica.

Note

When the status for a DB instance is `deleting`, its CA certificate value doesn't appear in the RDS console or in output for AWS CLI commands or RDS API operations. For more information about CA certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

Deletion protection

You can only delete instances that don't have deletion protection enabled. When you create or modify a DB instance, you have the option to enable deletion protection so that users can't delete the DB instance. Deletion protection is disabled by default for you when you use AWS CLI and API commands. Deletion protection is enabled for you when you use the AWS Management Console to create a production DB instance. However, Amazon RDS enforces deletion protection when you use the console, the CLI, or the API to delete a DB instance. To delete a DB instance that has deletion protection enabled, first modify the instance and disable deletion protection. Enabling or disabling deletion protection doesn't cause an outage.

Creating a final snapshot and retaining automated backups

When you delete a DB instance, you can choose to do one or both of the following:

- Create a final DB snapshot.
 - To be able to restore your deleted DB instance later, create a final DB snapshot. The final snapshot is retained, along with any manual snapshots that were taken.
 - To delete a DB instance quickly, you can skip creating a final DB snapshot.

Note

You can't create a final DB snapshot of your DB instance if it has the status `creating`, `failed`, `incompatible-restore`, or `incompatible-network`. For more information, see [Viewing Amazon RDS DB instance status \(p. 516\)](#).

- Retain automated backups.
 - Your automated backups are retained for the retention period that is set on the DB instance at the time when you delete it. This set retention period occurs whether or not you choose to create a final DB snapshot.
 - If you don't choose to retain automated backups, your automated backups in the same AWS Region as the DB instance are deleted. They can't be recovered after you delete the DB instance.

Note

Automated backups that are replicated to another AWS Region are retained even if you choose not to retain automated backups. For more information, see [Replicating automated backups to another AWS Region \(p. 437\)](#).

- You typically don't need to retain automated backups if you create a final DB snapshot.
- To delete a retained automated backup, follow the instructions in [Deleting retained automated backups \(p. 433\)](#).

Important

If you skip the final DB snapshot, to restore your DB instance do one of the following:

- Use an earlier manual snapshot of the DB instance to restore the DB instance to that DB snapshot's point in time.
- Retain automated backups. You can use them to restore your DB instance during your retention period, but not after your retention period has ended.

Note

Regardless of your choice, manual DB snapshots aren't deleted. For more information on snapshots, see [Creating a DB snapshot \(p. 448\)](#).

Deleting a DB instance

You can delete a DB instance using the AWS Management Console, the AWS CLI, or the RDS API.

The time required to delete a DB instance can vary depending on the backup retention period (that is, how many backups to delete), how much data is deleted, and whether a final snapshot is taken.

Note

You can't delete a DB instance when deletion protection is enabled for it. For more information, see [Deletion protection \(p. 421\)](#).

You can disable deletion protection by modifying the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Console

To delete a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to delete.
3. For **Actions**, choose **Delete**.
4. To create a final DB snapshot for the DB instance, choose **Create final snapshot?**.
5. If you chose to create a final snapshot, enter the **Final snapshot name**.
6. To retain automated backups, choose **Retain automated backups**.
7. Enter **delete me** in the box.
8. Choose **Delete**.

AWS CLI

To delete a DB instance by using the AWS CLI, call the `delete-db-instance` command with the following options:

- `--db-instance-identifier`

- `--final-db-snapshot-identifier` or `--skip-final-snapshot`

Example With a final snapshot and no retained automated backups

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \
  --db-instance-identifier mydbinstance \
  --final-db-snapshot-identifier mydbinstancefinalsnapshot \
  --delete-automated-backups
```

For Windows:

```
aws rds delete-db-instance ^
  --db-instance-identifier mydbinstance ^
  --final-db-snapshot-identifier mydbinstancefinalsnapshot ^
  --delete-automated-backups
```

Example With retained automated backups and no final snapshot

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \
  --db-instance-identifier mydbinstance \
  --skip-final-snapshot \
  --no-delete-automated-backups
```

For Windows:

```
aws rds delete-db-instance ^
  --db-instance-identifier mydbinstance ^
  --skip-final-snapshot ^
  --no-delete-automated-backups
```

RDS API

To delete a DB instance by using the Amazon RDS API, call the [DeleteDBInstance](#) operation with the following parameters:

- `DBInstanceIdentifier`
- `FinalDBSnapshotIdentifier` or `SkipFinalSnapshot`

Deleting a Multi-AZ DB cluster

You can delete a DB Multi-AZ DB cluster using the AWS Management Console, the AWS CLI, or the RDS API.

The time required to delete a Multi-AZ DB cluster can vary depending on certain factors. These are the backup retention period (that is, how many backups to delete), how much data is deleted, and whether a final snapshot is taken.

You can't delete a Multi-AZ DB cluster when deletion protection is turned on for it. For more information, see [Deletion protection \(p. 421\)](#). You can turn off deletion protection by modifying the Multi-AZ DB cluster. For more information, see [Modifying a Multi-AZ DB cluster \(p. 341\)](#).

Console

To delete a Multi-AZ DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the Multi-AZ DB cluster that you want to delete.
3. For **Actions**, choose **Delete**.
4. Choose **Create final snapshot?** to create a final DB snapshot for the Multi-AZ DB cluster.
If you create a final snapshot, enter a name for **Final snapshot name**.
5. Choose **Retain automated backups** to retain automated backups.
6. Enter **delete me** in the box.
7. Choose **Delete**.

AWS CLI

To delete a Multi-AZ DB cluster by using the AWS CLI, call the `delete-db-cluster` command with the following options:

- `--db-cluster-identifier`
- `--final-db-snapshot-identifier` or `--skip-final-snapshot`

Example With a final snapshot

For Linux, macOS, or Unix:

```
aws rds delete-db-cluster \
--db-cluster-identifier mymultiazdbcluster \
--final-db-snapshot-identifier mymultiazdbclusterfinalsnapshot
```

For Windows:

```
aws rds delete-db-cluster ^
--db-cluster-identifier mymultiazdbcluster ^
--final-db-snapshot-identifier mymultiazdbclusterfinalsnapshot
```

Example With no final snapshot

For Linux, macOS, or Unix:

```
aws rds delete-db-cluster \
--db-cluster-identifier mymultiazdbcluster \
--skip-final-snapshot
```

For Windows:

```
aws rds delete-db-cluster ^
--db-cluster-identifier mymultiazdbcluster ^
--skip-final-snapshot
```

RDS API

To delete a Multi-AZ DB cluster by using the Amazon RDS API, call the [DeleteDBCluster](#) operation with the following parameters:

- `DBClusterIdentifier`
- `FinalDBSnapshotIdentifier` or `SkipFinalSnapshot`

Backing up and restoring an Amazon RDS DB instance

This section shows how to back up and restore a DB instance.

Topics

- [Working with backups \(p. 427\)](#)
- [Replicating automated backups to another AWS Region \(p. 437\)](#)
- [Creating a DB snapshot \(p. 448\)](#)
- [Creating a Multi-AZ DB cluster snapshot \(p. 450\)](#)
- [Restoring from a DB snapshot \(p. 452\)](#)
- [Restoring from a snapshot to a Multi-AZ DB cluster \(p. 456\)](#)
- [Copying a DB snapshot \(p. 458\)](#)
- [Sharing a DB snapshot \(p. 472\)](#)
- [Exporting DB snapshot data to Amazon S3 \(p. 481\)](#)
- [Restoring a DB instance to a specified time \(p. 499\)](#)
- [Restoring a Multi-AZ DB cluster to a specified time \(p. 502\)](#)
- [Deleting a DB snapshot \(p. 505\)](#)
- [Tutorial: Restore an Amazon RDS DB instance from a DB snapshot \(p. 507\)](#)

Working with backups

Amazon RDS creates and saves automated backups of your DB instance during the backup window of your DB instance. RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. RDS saves the automated backups of your DB instance according to the backup retention period that you specify. If necessary, you can recover your database to any point in time during the backup retention period.

Automated backups follow these rules:

- Your DB instance must be in the available state for automated backups to occur. Automated backups don't occur while your DB instance is in a state other than available, for example `storage_full`.
- Automated backups don't occur while a DB snapshot copy is running in the same AWS Region for the same DB instance.

You can also back up your DB instance manually, by manually creating a DB snapshot. For more information about creating a DB snapshot, see [Creating a DB snapshot \(p. 448\)](#).

The first snapshot of a DB instance contains the data for the full DB instance. Subsequent snapshots of the same DB instance are incremental, which means that only the data that has changed after your most recent snapshot is saved.

You can copy both automatic and manual DB snapshots, and share manual DB snapshots. For more information about copying a DB snapshot, see [Copying a DB snapshot \(p. 458\)](#). For more information about sharing a DB snapshot, see [Sharing a DB snapshot \(p. 472\)](#).

Topics

- [Backup storage \(p. 427\)](#)
- [Backup window \(p. 428\)](#)
- [Backup retention period \(p. 429\)](#)
- [Enabling automated backups \(p. 429\)](#)
- [Retaining automated backups \(p. 431\)](#)
- [Deleting retained automated backups \(p. 433\)](#)
- [Disabling automated backups \(p. 434\)](#)
- [Using AWS Backup to manage automated backups \(p. 435\)](#)
- [Automated backups with unsupported MySQL storage engines \(p. 435\)](#)
- [Automated backups with unsupported MariaDB storage engines \(p. 436\)](#)

Backup storage

Your Amazon RDS backup storage for each AWS Region is composed of the automated backups and manual DB snapshots for that Region. Total backup storage space equals the sum of the storage for all backups in that Region. Moving a DB snapshot to another Region increases the backup storage in the destination Region. Backups are stored in Amazon S3.

For more information about backup storage costs, see [Amazon RDS pricing](#).

If you chose to retain automated backups when you delete a DB instance, the automated backups are saved for the full retention period. If you don't choose **Retain automated backups** when you delete a DB instance, all automated backups are deleted with the DB instance. After they are deleted, the automated backups can't be recovered. If you choose to have Amazon RDS create a final DB snapshot before it

deletes your DB instance, you can use that to recover your DB instance. Or you can use a previously created manual snapshot. Manual snapshots are not deleted. You can have up to 100 manual snapshots per Region.

Backup window

Automated backups occur daily during the preferred backup window. If the backup requires more time than allotted to the backup window, the backup continues after the window ends, until it finishes. The backup window can't overlap with the weekly maintenance window for the DB instance.

During the automatic backup window, storage I/O might be suspended briefly while the backup process initializes (typically under a few seconds). You might experience elevated latencies for a few minutes during backups for Multi-AZ deployments. For MariaDB, MySQL, Oracle, and PostgreSQL, I/O activity isn't suspended on your primary during backup for Multi-AZ deployments, because the backup is taken from the standby. For SQL Server, I/O activity is suspended briefly during backup for both Single-AZ and Multi-AZ deployments, because the backup is taken from the primary.

Automated backups might occasionally be skipped if the DB instance has a heavy workload at the time a backup is supposed to start. If a backup is skipped, you can still do a point-in-time-recovery (PITR), and a backup is still attempted during the next backup window. For more information on PITR, see [Restoring a DB instance to a specified time \(p. 499\)](#).

If you don't specify a preferred backup window when you create the DB instance, Amazon RDS assigns a default 30-minute backup window. This window is selected at random from an 8-hour block of time for each AWS Region. The following table lists the time blocks for each AWS Region from which the default backup windows are assigned.

Region Name	Region	Time Block
US East (Ohio)	us-east-2	03:00–11:00 UTC
US East (N. Virginia)	us-east-1	03:00–11:00 UTC
US West (N. California)	us-west-1	06:00–14:00 UTC
US West (Oregon)	us-west-2	06:00–14:00 UTC
Africa (Cape Town)	af-south-1	03:00–11:00 UTC
Asia Pacific (Hong Kong)	ap-east-1	06:00–14:00 UTC
Asia Pacific (Hyderabad)	ap-south-2	06:30–14:30 UTC
Asia Pacific (Jakarta)	ap-southeast-3	08:00–16:00 UTC
Asia Pacific (Mumbai)	ap-south-1	16:30–00:30 UTC
Asia Pacific (Osaka)	ap-northeast-3	00:00–08:00 UTC
Asia Pacific (Seoul)	ap-northeast-2	13:00–21:00 UTC
Asia Pacific (Singapore)	ap-southeast-1	14:00–22:00 UTC
Asia Pacific (Sydney)	ap-southeast-2	12:00–20:00 UTC
Asia Pacific (Tokyo)	ap-northeast-1	13:00–21:00 UTC
Canada (Central)	ca-central-1	03:00–11:00 UTC

Region Name	Region	Time Block
China (Beijing)	cn-north-1	06:00–14:00 UTC
China (Ningxia)	cn-northwest-1	06:00–14:00 UTC
Europe (Frankfurt)	eu-central-1	20:00–04:00 UTC
Europe (Ireland)	eu-west-1	22:00–06:00 UTC
Europe (London)	eu-west-2	22:00–06:00 UTC
Europe (Milan)	eu-south-1	02:00–10:00 UTC
Europe (Paris)	eu-west-3	07:29–14:29 UTC
Europe (Spain)	eu-south-2	02:00–10:00 UTC
Europe (Stockholm)	eu-north-1	23:00–07:00 UTC
Europe (Zurich)	eu-central-2	02:00–10:00 UTC
Middle East (Bahrain)	me-south-1	06:00–14:00 UTC
Middle East (UAE)	me-central-1	05:00–13:00 UTC
South America (São Paulo)	sa-east-1	23:00–07:00 UTC
AWS GovCloud (US-East)	us-gov-east-1	17:00–01:00 UTC
AWS GovCloud (US-West)	us-gov-west-1	06:00–14:00 UTC

Backup retention period

You can set the backup retention period when you create a DB instance. If you don't set the backup retention period, the default backup retention period is one day if you create the DB instance using the Amazon RDS API or the AWS CLI. The default backup retention period is seven days if you create the DB instance using the console.

After you create a DB instance, you can modify the backup retention period. You can set the backup retention period to between 0 and 35 days. Setting the backup retention period to 0 disables automated backups. Manual snapshot limits (100 per Region) do not apply to automated backups.

Automated backups aren't created while a DB instance is stopped. Backups can be retained longer than the backup retention period if a DB instance has been stopped. RDS doesn't include time spent in the stopped state when the backup retention window is calculated.

Important

An outage occurs if you change the backup retention period from 0 to a nonzero value or from a nonzero value to 0. This applies to both Single-AZ and Multi-AZ DB instances.

Enabling automated backups

If your DB instance doesn't have automated backups enabled, you can enable them at any time. You enable automated backups by setting the backup retention period to a positive nonzero value. When

automated backups are enabled, your RDS instance and database is taken offline and a backup is immediately created.

Note

If you manage your backups in AWS Backup, you can't enable automated backups. For more information, see [Using AWS Backup to manage automated backups \(p. 435\)](#).

Console

To enable automated backups immediately

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **Backup retention period**, choose a positive nonzero value, for example 3 days.
5. Choose **Continue**.
6. Choose **Apply immediately**.
7. On the confirmation page, choose **Modify DB instance** to save your changes and enable automated backups.

AWS CLI

To enable automated backups, use the AWS CLI `modify-db-instance` command.

Include the following parameters:

- `--db-instance-identifier`
- `--backup-retention-period`
- `--apply-immediately` or `--no-apply-immediately`

In the following example, we enable automated backups by setting the backup retention period to three days. The changes are applied immediately.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --backup-retention-period 3 \
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --backup-retention-period 3 ^
  --apply-immediately
```

RDS API

To enable automated backups, use the RDS API `ModifyDBInstance` operation with the following required parameters:

- `DBInstanceIdentifier`
- `BackupRetentionPeriod`

Viewing automated backups

To view your automated backups, choose **Automated backups** in the navigation pane. To view individual snapshots associated with an automated backup, choose **Snapshots** in the navigation pane. Alternatively, you can describe individual snapshots associated with an automated backup. From there, you can restore a DB instance directly from one of those snapshots.

To describe the automated backups for your existing DB instances using the AWS CLI, use one of the following commands:

```
aws rds describe-db-instance-automated-backups --db-instance-  
identifier DBInstanceIdentifier
```

or

```
aws rds describe-db-instance-automated-backups --dbi-resource-id DbiResourceId
```

To describe the retained automated backups for your existing DB instances using the RDS API, call the [DescribeDBInstanceAutomatedBackups](#) action with one of the following parameters:

- `DBInstanceIdentifier`
- `DbiResourceId`

Retaining automated backups

When you delete a DB instance, you can retain automated backups.

Retained automated backups contain system snapshots and transaction logs from a DB instance. They also include your DB instance properties like allocated storage and DB instance class, which are required to restore it to an active instance.

You can retain automated backups for RDS instances running the MySQL, MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server engines.

You can restore or remove retained automated backups using the AWS Management Console, RDS API, and AWS CLI.

Topics

- [Retention period \(p. 431\)](#)
- [Viewing retained backups \(p. 432\)](#)
- [Restoration \(p. 432\)](#)
- [Retention costs \(p. 432\)](#)
- [Limitations and recommendations \(p. 432\)](#)

Retention period

The system snapshots and transaction logs in a retained automated backup expire the same way that they expire for the source DB instance. Because there are no new snapshots or logs created for this

instance, the retained automated backups eventually expire completely. Effectively, they live as long their last system snapshot would have done, based on the settings for retention period the source instance had when you deleted it. Retained automated backups are removed by the system after their last system snapshot expires.

You can remove a retained automated backup in the same way that you can delete a DB instance. You can remove retained automated backups using the console or the RDS API operation `DeleteDBInstanceAutomatedBackup`.

Final snapshots are independent of retained automated backups. We strongly suggest that you take a final snapshot even if you retain automated backups, because the retained automated backups eventually expire. The final snapshot doesn't expire.

Viewing retained backups

To view your retained automated backups, choose **Automated backups** in the navigation pane, then choose **Retained**. To view individual snapshots associated with a retained automated backup, choose **Snapshots** in the navigation pane. Alternatively, you can describe individual snapshots associated with a retained automated backup. From there, you can restore a DB instance directly from one of those snapshots.

To describe your retained automated backups using the AWS CLI, use the following command:

```
aws rds describe-db-instance-automated-backups --dbi-resource-id DbiResourceId
```

To describe your retained automated backups using the RDS API, call the [DescribeDBInstanceAutomatedBackups](#) action with the `DbiResourceId` parameter.

Restoration

For information on restoring DB instances from automated backups, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Retention costs

The cost of a retained automated backup is the cost of total storage of the system snapshots that are associated with it. There is no additional charge for transaction logs or instance metadata. All other pricing rules for backups apply to restorable instances.

For example, suppose that your total allocated storage of running instances is 100 GB. Suppose also that you have 50 GB of manual snapshots plus 75 GB of system snapshots associated with a retained automated backup. In this case, you are charged only for the additional 25 GB of backup storage, like this: $(50 \text{ GB} + 75 \text{ GB}) - 100 \text{ GB} = 25 \text{ GB}$.

Limitations and recommendations

The following limitations apply to retained automated backups:

- The maximum number of retained automated backups in one AWS Region is 40. It's not included in the DB instances limit. You can have 40 running DB instances and an additional 40 retained automated backups at the same time.
- Retained automated backups don't contain information about parameters or option groups.
- You can restore a deleted instance to a point in time that is within the retention period at the time of delete.

- You can't modify a retained automated backup. That's because it consists of system backups, transaction logs, and the DB instance properties that existed at the time that you deleted the source instance.

Deleting retained automated backups

You can delete retained automated backups when they are no longer needed.

Console

To delete a retained automated backup

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Automated backups**.
3. On the **Retained** tab, choose the retained automated backup that you want to delete.
4. For **Actions**, choose **Delete**.
5. On the confirmation page, enter **delete me** and choose **Delete**.

AWS CLI

You can delete a retained automated backup by using the AWS CLI command `delete-db-instance-automated-backup` with the following option:

- `--dbi-resource-id` – The resource identifier for the source DB instance.

You can find the resource identifier for the source DB instance of a retained automated backup by running the AWS CLI command `describe-db-instance-automated-backups`.

Example

The following example deletes the retained automated backup with source DB instance resource identifier db-123ABCEXAMPLE.

For Linux, macOS, or Unix:

```
aws rds delete-db-instance-automated-backup \
--dbi-resource-id db-123ABCEXAMPLE
```

For Windows:

```
aws rds delete-db-instance-automated-backup ^
--dbi-resource-id db-123ABCEXAMPLE
```

RDS API

You can delete a retained automated backup by using the Amazon RDS API operation `DeleteDBInstanceAutomatedBackup` with the following parameter:

- `DbiResourceId` – The resource identifier for the source DB instance.

You can find the resource identifier for the source DB instance of a retained automated backup using the Amazon RDS API operation `DescribeDBInstanceAutomatedBackups`.

Disabling automated backups

You might want to temporarily disable automated backups in certain situations, for example while loading large amounts of data.

Important

We highly discourage disabling automated backups because it disables point-in-time recovery. Disabling automatic backups for a DB instance deletes all existing automated backups for the instance. If you disable and then re-enable automated backups, you can restore starting only from the time you re-enabled automated backups.

Console

To disable automated backups immediately

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **Backup retention period**, choose **0 days**.
5. Choose **Continue**.
6. Choose **Apply immediately**.
7. On the confirmation page, choose **Modify DB instance** to save your changes and disable automated backups.

AWS CLI

To disable automated backups immediately, use the `modify-db-instance` command and set the backup retention period to 0 with `--apply-immediately`.

Example

The following example immediately disabled automatic backups.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --backup-retention-period 0 \
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --backup-retention-period 0 ^
  --apply-immediately
```

To know when the modification is in effect, call `describe-db-instances` for the DB instance until the value for backup retention period is 0 and `mydbinstance` status is available.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

RDS API

To disable automated backups immediately, call the [ModifyDBInstance](#) operation with the following parameters:

- DBInstanceIdentifier = mydbinstance
- BackupRetentionPeriod = 0

Example

```
https://rds.amazonaws.com/  
    ?Action=ModifyDBInstance  
    &DBInstanceIdentifier=mydbinstance  
    &BackupRetentionPeriod=0  
    &SignatureVersion=2  
    &SignatureMethod=HmacSHA256  
    &Timestamp=2009-10-14T17%3A48%3A21.746Z  
    &AWSAccessKeyId=<&AWS; Access Key ID>  
    &Signature=<Signature>
```

Using AWS Backup to manage automated backups

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises. You can manage backups of your Amazon RDS DB instances in AWS Backup.

To enable backups in AWS Backup, you use resource tagging to associate your DB instance with a backup plan. For more information, see [Using tags to enable backups in AWS Backup \(p. 399\)](#).

Note

Backups managed by AWS Backup are considered manual DB snapshots, but don't count toward the DB snapshot quota for RDS. Backups that were created with AWS Backup have names ending in awsbackup:*backup-job-number*.

For more information about AWS Backup, see the [AWS Backup Developer Guide](#).

To view backups managed by AWS Backup

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the **Backup service** tab.

Your AWS Backup backups are listed under **Backup service snapshots**.

Automated backups with unsupported MySQL storage engines

For the MySQL DB engine, automated backups are only supported for the InnoDB storage engine. Use of these features with other MySQL storage engines, including MyISAM, can lead to unreliable behavior while restoring from backups. Specifically, since storage engines like MyISAM don't support reliable crash recovery, your tables can be corrupted in the event of a crash. For this reason, we encourage you to use the InnoDB storage engine.

- To convert existing MyISAM tables to InnoDB tables, you can use the ALTER TABLE command, for example: ALTER TABLE *table_name* ENGINE=innodb, ALGORITHM=COPY;
- If you choose to use MyISAM, you can attempt to manually repair tables that become damaged after a crash by using the REPAIR command. For more information, see [REPAIR TABLE statement](#) in the MySQL documentation. However, as noted in the MySQL documentation, there is a good chance that you might not be able to recover all your data.
- If you want to take a snapshot of your MyISAM tables before restoring, follow these steps:
 1. Stop all activity to your MyISAM tables (that is, close all sessions).

You can close all sessions by calling the `mysql.rds_kill` command for each process that is returned from the `SHOW FULL PROCESSLIST` command.

2. Lock and flush each of your MyISAM tables. For example, the following commands lock and flush two tables named `myisam_table1` and `myisam_table2`:

```
mysql> FLUSH TABLES myisam_table1, myisam_table2 WITH READ LOCK;
```

3. Create a snapshot of your DB instance. When the snapshot has completed, release the locks and resume activity on the MyISAM tables. You can release the locks on your tables using the following command:

```
mysql> UNLOCK TABLES;
```

These steps force MyISAM to flush data stored in memory to disk, which ensures a clean start when you restore from a DB snapshot. For more information on creating a DB snapshot, see [Creating a DB snapshot \(p. 448\)](#).

Automated backups with unsupported MariaDB storage engines

For the MariaDB DB engine, automated backups are only supported with the InnoDB storage engine. Use of these features with other MariaDB storage engines, including Aria, might lead to unreliable behavior while restoring from backups. Even though Aria is a crash-resistant alternative to MyISAM, your tables can still be corrupted in the event of a crash. For this reason, we encourage you to use the InnoDB storage engine.

- To convert existing Aria tables to InnoDB tables, you can use the ALTER TABLE command. For example: ALTER TABLE *table_name* ENGINE=innodb, ALGORITHM=COPY;
- If you choose to use Aria, you can attempt to manually repair tables that become damaged after a crash by using the REPAIR TABLE command. For more information, see <http://mariadb.com/kb/en/mariadb/repair-table/>.
- If you want to take a snapshot of your Aria tables before restoring, follow these steps:
 1. Stop all activity to your Aria tables (that is, close all sessions).
 2. Lock and flush each of your Aria tables.
 3. Create a snapshot of your DB instance. When the snapshot has completed, release the locks and resume activity on the Aria tables. These steps force Aria to flush data stored in memory to disk, thereby ensuring a clean start when you restore from a DB snapshot.

Replicating automated backups to another AWS Region

For added disaster recovery capability, you can configure your Amazon RDS database instance to replicate snapshots and transaction logs to a destination AWS Region of your choice. When backup replication is configured for a DB instance, RDS initiates a cross-Region copy of all snapshots and transaction logs as soon as they are ready on the DB instance.

DB snapshot copy charges apply to the data transfer. After the DB snapshot is copied, standard charges apply to storage in the destination Region. For more details, see [RDS Pricing](#).

For an example of using backup replication, see the AWS online tech talk [Managed Disaster Recovery with Amazon RDS for Oracle Cross-Region Automated Backups](#).

Topics

- [Region and version availability \(p. 437\)](#)
- [Source and destination AWS Region support \(p. 437\)](#)
- [Enabling cross-Region automated backups \(p. 439\)](#)
- [Finding information about replicated backups \(p. 441\)](#)
- [Restoring to a specified time from a replicated backup \(p. 444\)](#)
- [Stopping automated backup replication \(p. 445\)](#)
- [Deleting replicated backups \(p. 446\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability with cross-Region automated backups, see [Cross-Region automated backups \(p. 78\)](#).

Source and destination AWS Region support

Backup replication is supported between the following AWS Regions.

Source Region	Destination Regions available
Asia Pacific (Mumbai)	Asia Pacific (Singapore) US East (N. Virginia), US East (Ohio), US West (Oregon)
Asia Pacific (Osaka)	Asia Pacific (Tokyo)
Asia Pacific (Seoul)	Asia Pacific (Singapore), Asia Pacific (Tokyo) US East (N. Virginia), US East (Ohio), US West (Oregon)
Asia Pacific (Singapore)	Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Sydney), Asia Pacific (Tokyo) US East (N. Virginia), US East (Ohio), US West (Oregon)
Asia Pacific (Sydney)	Asia Pacific (Singapore) US East (N. Virginia), US West (N. California), US West (Oregon)

Source Region	Destination Regions available
Asia Pacific (Tokyo)	Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Singapore) US East (N. Virginia), US East (Ohio), US West (Oregon)
Canada (Central)	Europe (Ireland) US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon)
China (Beijing)	China (Ningxia)
China (Ningxia)	China (Beijing)
Europe (Frankfurt)	Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm) US East (N. Virginia), US East (Ohio), US West (Oregon)
Europe (Ireland)	Canada (Central) Europe (Frankfurt), Europe (London), Europe (Paris), Europe (Stockholm) US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon)
Europe (London)	Europe (Frankfurt), Europe (Ireland), Europe (Paris), Europe (Stockholm) US East (N. Virginia)
Europe (Paris)	Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Stockholm) US East (N. Virginia)
Europe (Stockholm)	Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris) US East (N. Virginia)
South America (São Paulo)	US East (N. Virginia), US East (Ohio)
AWS GovCloud (US-East)	AWS GovCloud (US-West)
AWS GovCloud (US-West)	AWS GovCloud (US-East)
US East (N. Virginia)	Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo) Canada (Central) Europe (Frankfurt), Europe (Ireland), Europe (London), Europe (Paris), Europe (Stockholm) South America (São Paulo) US East (Ohio), US West (N. California), US West (Oregon)

Source Region	Destination Regions available
US East (Ohio)	Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Tokyo) Canada (Central) Europe (Frankfurt), Europe (Ireland) South America (São Paulo) US East (N. Virginia), US West (N. California), US West (Oregon)
US West (N. California)	Asia Pacific (Sydney) Canada (Central) Europe (Ireland) US East (N. Virginia), US East (Ohio), US West (Oregon)
US West (Oregon)	Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo) Canada (Central) Europe (Frankfurt), Europe (Ireland) US East (N. Virginia), US East (Ohio), US West (N. California)

You can also use the `describe-source-regions` AWS CLI command to find out which AWS Regions can replicate to each other. For more information, see [Finding information about replicated backups \(p. 441\)](#).

Enabling cross-Region automated backups

You can enable backup replication on new or existing DB instances using the Amazon RDS console. You can also use the `start-db-instance-automated-backups-replication` AWS CLI command or the `StartDBInstanceAutomatedBackupsReplication` RDS API operation. You can replicate up to 20 backups to each destination AWS Region for each AWS account.

Note

To be able to replicate automated backups, make sure to enable them. For more information, see [Enabling automated backups \(p. 429\)](#).

Console

You can enable backup replication for a new or existing DB instance:

- For a new DB instance, enable it when you launch the instance. For more information, see [Settings for DB instances \(p. 237\)](#).
- For an existing DB instance, use the following procedure.

To enable backup replication for an existing DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Automated backups**.
3. On the **Current Region** tab, choose the DB instance for which you want to enable backup replication.
4. For **Actions**, choose **Manage cross-Region replication**.
5. Under **Backup replication**, choose **Enable replication to another AWS Region**.
6. Choose the **Destination Region**.
7. Choose the **Replicated backup retention period**.
8. If you've enabled encryption on the source DB instance, choose the **AWS KMS key** for encrypting the backups.
9. Choose **Save**.

In the source Region, replicated backups are listed on the **Current Region** tab of the **Automated backups** page. In the destination Region, replicated backups are listed on the **Replicated backups** tab of the **Automated backups** page.

AWS CLI

Enable backup replication by using the [start-db-instance-automated-backups-replication](#) AWS CLI command.

The following CLI example replicates automated backups from a DB instance in the US West (Oregon) Region to the US East (N. Virginia) Region. It also encrypts the replicated backups, using an AWS KMS key in the destination Region.

To enable backup replication

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds start-db-instance-automated-backups-replication \
--region us-east-1 \
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase" \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE" \
--backup-retention-period 7
```

For Windows:

```
aws rds start-db-instance-automated-backups-replication ^
--region us-east-1 ^
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase" ^
--kms-key-id "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE" ^
--backup-retention-period 7
```

The **--source-region** option is required when you encrypt backups between the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. For **--source-region**, specify the AWS Region of the source DB instance.

If **--source-region** isn't specified, make sure to specify a **--pre-signed-url** value. A *presigned URL* is a URL that contains a Signature Version 4 signed request for the `start-db-instance-automated-backups-replication` command that is called in the source AWS Region. To learn more about the **pre-signed-url** option, see [start-db-instance-automated-backups-replication](#) in the [AWS CLI Command Reference](#).

RDS API

Enable backup replication by using the [StartDBInstanceAutomatedBackupsReplication](#) RDS API operation with the following parameters:

- Region
- SourceDBInstanceArn
- BackupRetentionPeriod
- KmsKeyId (optional)
- PreSignedUrl (required if you use KmsKeyId)

Note

If you encrypt the backups, you must also include a presigned URL. For more information on presigned URLs, see [Authenticating Requests: Using Query Parameters \(AWS Signature Version 4\)](#) in the *Amazon Simple Storage Service API Reference* and [Signature Version 4 signing process](#) in the *AWS General Reference*.

Finding information about replicated backups

You can use the following CLI commands to find information about replicated backups:

- `describe-source-regions`
- `describe-db-instances`
- `describe-db-instance-automated-backups`

The following `describe-source-regions` example lists the source AWS Regions from which automated backups can be replicated to the US West (Oregon) destination Region.

To show information about source Regions

- Run the following command.

```
aws rds describe-source-regions --region us-west-2
```

The output shows that backups can be replicated from US East (N. Virginia), but not from US East (Ohio) or US West (N. California), into US West (Oregon).

```
{  
    "SourceRegions": [  
        ...  
        {  
            "RegionName": "us-east-1",  
            "Endpoint": "https://rds.us-east-1.amazonaws.com",  
            "Status": "available",  
            "SupportsDBInstanceAutomatedBackupsReplication": true  
        },  
        {  
            "RegionName": "us-east-2",  
            "Endpoint": "https://rds.us-east-2.amazonaws.com",  
            "Status": "available",  
            "SupportsDBInstanceAutomatedBackupsReplication": false  
        },  
        "RegionName": "us-west-1",  
        "Endpoint": "https://rds.us-west-1.amazonaws.com",  
        "Status": "available",  
        "SupportsDBInstanceAutomatedBackupsReplication": true  
    ]  
}
```

```
        "Status": "available",
        "SupportsDBInstanceAutomatedBackupsReplication": false
    ]
}
```

The following `describe-db-instances` example shows the automated backups for a DB instance.

To show the replicated backups for a DB instance

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds describe-db-instances \
--db-instance-identifier mydatabase
```

For Windows:

```
aws rds describe-db-instances ^
--db-instance-identifier mydatabase
```

The output includes the replicated backups.

```
{
    "DBInstances": [
        {
            "StorageEncrypted": false,
            "Endpoint": {
                "HostedZoneId": "Z1PVIF0B656C1W",
                "Port": 1521,
                ...
                "BackupRetentionPeriod": 7,
                "DBInstanceAutomatedBackupsReplications": [{"DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7H0J4SIEEXAMPLE"}]
            }
        ]
    }
}
```

The following `describe-db-instance-automated-backups` example shows the automated backups for a DB instance.

To show automated backups for a DB instance

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds describe-db-instance-automated-backups \
--db-instance-identifier mydatabase
```

For Windows:

```
aws rds describe-db-instance-automated-backups ^
--db-instance-identifier mydatabase
```

The output shows the source DB instance and automated backups in US West (Oregon), with backups replicated to US East (N. Virginia).

```
{
    "DBInstanceAutomatedBackups": [
        {
            "DBInstanceArn": "arn:aws:rds:us-west-2:868710585169:db:mydatabase",
            "DbiResourceId": "db-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE",
            "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-west-2:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE",
            "BackupRetentionPeriod": 7,
            "DBInstanceAutomatedBackupsReplications": [{"DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE"}]
            "Region": "us-west-2",
            "DBInstanceIdentifier": "mydatabase",
            "RestoreWindow": {
                "EarliestTime": "2020-10-26T01:09:07Z",
                "LatestTime": "2020-10-31T19:09:53Z",
            }
            ...
        }
    ]
}
```

The following `describe-db-instance-automated-backups` example uses the `--db-instance-automated-backups-arn` option to show the replicated backups in the destination Region.

To show replicated backups

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds describe-db-instance-automated-backups \
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE"
```

For Windows:

```
aws rds describe-db-instance-automated-backups ^
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE"
```

The output shows the source DB instance in US West (Oregon), with replicated backups in US East (N. Virginia).

```
{
    "DBInstanceAutomatedBackups": [
        {
            "DBInstanceArn": "arn:aws:rds:us-west-2:868710585169:db:mydatabase",
            "DbiResourceId": "db-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE",
            "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEEXAMPLE",
            "Region": "us-west-2",
            "DBInstanceIdentifier": "mydatabase",
            "RestoreWindow": {
                "EarliestTime": "2020-10-26T01:09:07Z",
                "LatestTime": "2020-10-31T19:01:23Z"
            },
        }
    ]
}
```

```
        "AllocatedStorage": 50,  
        "BackupRetentionPeriod": 7,  
        "Status": "replicating",  
        "Port": 1521,  
        ...  
    ]  
}
```

Restoring to a specified time from a replicated backup

You can restore a DB instance to a specific point in time from a replicated backup using the Amazon RDS console. You can also use the `restore-db-instance-to-point-in-time` AWS CLI command or the `RestoreDBInstanceToPointInTime` RDS API operation.

For general information on point-in-time recovery (PITR), see [Restoring a DB instance to a specified time \(p. 499\)](#).

Note

On RDS for SQL Server, option groups aren't copied across AWS Regions when automated backups are replicated. If you've associated a custom option group with your RDS for SQL Server DB instance, you can re-create that option group in the destination Region. Then restore the DB instance in the destination Region and associate the custom option group with it. For more information, see [Working with option groups \(p. 273\)](#).

Console

To restore a DB instance to a specified time from a replicated backup

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose the destination Region (where backups are replicated to) from the Region selector.
3. In the navigation pane, choose **Automated backups**.
4. On the **Replicated backups** tab, choose the DB instance that you want to restore.
5. For **Actions**, choose **Restore to point in time**.
6. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time that you want to restore the instance to.

Note

Times are shown in your local time zone, which is indicated by an offset from Coordinated Universal Time (UTC). For example, UTC-5 is Eastern Standard Time/Central Daylight Time.

7. For **DB instance identifier**, enter the name of the target restored DB instance.
8. (Optional) Choose other options as needed, such as enabling autoscaling.
9. Choose **Restore to point in time**.

AWS CLI

Use the `restore-db-instance-to-point-in-time` AWS CLI command to create a new DB instance.

To restore a DB instance to a specified time from a replicated backup

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-automated-backups-arn "arn:aws:rds:us-
east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7H0J4SIEEXAMPLE" \
    --target-db-instance-identifier mytargetdbinstance \
    --restore-time 2020-10-14T23:45:00.000Z
```

For Windows:

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-automated-backups-arn "arn:aws:rds:us-
east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7H0J4SIEEXAMPLE" ^
    --target-db-instance-identifier mytargetdbinstance ^
    --restore-time 2020-10-14T23:45:00.000Z
```

RDS API

To restore a DB instance to a specified time, call the [RestoreDBInstanceToPointInTime](#) Amazon RDS API operation with the following parameters:

- `SourceDBInstanceAutomatedBackupsArn`
- `TargetDBInstanceIdentifier`
- `RestoreTime`

Stopping automated backup replication

You can stop backup replication for DB instances using the Amazon RDS console. You can also use the `stop-db-instance-automated-backups-replication` AWS CLI command or the `StopDBInstanceAutomatedBackupsReplication` RDS API operation.

Replicated backups are retained, subject to the backup retention period set when they were created.

Console

Stop backup replication from the **Automated backups** page in the source Region.

To stop backup replication to an AWS Region

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose the source Region from the **Region selector**.
3. In the navigation pane, choose **Automated backups**.
4. On the **Current Region** tab, choose the DB instance for which you want to stop backup replication.
5. For **Actions**, choose **Manage cross-Region replication**.
6. Under **Backup replication**, clear the **Enable replication to another AWS Region** check box.
7. Choose **Save**.

Replicated backups are listed on the **Retained** tab of the **Automated backups** page in the destination Region.

AWS CLI

Stop backup replication by using the [stop-db-instance-automated-backups-replication](#) AWS CLI command.

The following CLI example stops automated backups of a DB instance from replicating in the US West (Oregon) Region.

To stop backup replication

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds stop-db-instance-automated-backups-replication \
--region us-east-1 \
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase"
```

For Windows:

```
aws rds stop-db-instance-automated-backups-replication ^
--region us-east-1 ^
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase"
```

RDS API

Stop backup replication by using the [StopDBInstanceAutomatedBackupsReplication](#) RDS API operation with the following parameters:

- Region
- SourceDBInstanceArn

Deleting replicated backups

You can delete replicated backups for DB instances using the Amazon RDS console. You can also use the `delete-db-instance-automated-backups` AWS CLI command or the `DeleteDBInstanceAutomatedBackup` RDS API operation.

Console

Delete replicated backups in the destination Region from the **Automated backups** page.

To delete replicated backups

- Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
- Choose the destination Region from the **Region selector**.
- In the navigation pane, choose **Automated backups**.
- On the **Replicated backups** tab, choose the DB instance for which you want to delete the replicated backups.
- For **Actions**, choose **Delete**.
- On the confirmation page, enter **delete me** and choose **Delete**.

AWS CLI

Delete replicated backups by using the [delete-db-instance-automated-backup](#) AWS CLI command.

You can use the [describe-db-instances](#) CLI command to find the Amazon Resource Names (ARNs) of the replicated backups. For more information, see [Finding information about replicated backups \(p. 441\)](#).

To delete replicated backups

- Run one of the following commands.

For Linux, macOS, or Unix:

```
aws rds delete-db-instance-automated-backup \
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-
L2IJCEXJP7XQ7H0J4SIEEXAMPLE"
```

For Windows:

```
aws rds delete-db-instance-automated-backup ^
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-
L2IJCEXJP7XQ7H0J4SIEEXAMPLE"
```

RDS API

Delete replicated backups by using the [DeleteDBInstanceAutomatedBackup](#) RDS API operation with the `DBInstanceAutomatedBackupsArn` parameter.

Creating a DB snapshot

Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. Creating this DB snapshot on a Single-AZ DB instance results in a brief I/O suspension that can last from a few seconds to a few minutes, depending on the size and class of your DB instance. For MariaDB, MySQL, Oracle, and PostgreSQL, I/O activity is not suspended on your primary during backup for Multi-AZ deployments, because the backup is taken from the standby. For SQL Server, I/O activity is suspended briefly during backup for Multi-AZ deployments.

When you create a DB snapshot, you need to identify which DB instance you are going to back up, and then give your DB snapshot a name so you can restore from it later. The amount of time it takes to create a snapshot varies with the size of your databases. Since the snapshot includes the entire storage volume, the size of files, such as temporary files, also affects the amount of time it takes to create the snapshot.

Note

Your DB instance must be in the available state to take a DB snapshot.

For PostgreSQL DB instances, data in unlogged tables might not be restored from snapshots.

For more information, see [Best practices for working with PostgreSQL \(p. 224\)](#).

Unlike automated backups, manual snapshots aren't subject to the backup retention period. Snapshots don't expire.

For very long-term backups of MariaDB, MySQL, and PostgreSQL data, we recommend exporting snapshot data to Amazon S3. If the major version of your DB engine is no longer supported, you can't restore to that version from a snapshot. For more information, see [Exporting DB snapshot data to Amazon S3 \(p. 481\)](#).

You can create a DB snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To create a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. In the list of DB instances, choose the DB instance for which you want to take a snapshot.
4. For **Actions**, choose **Take snapshot**.

The **Take DB snapshot** window appears.

5. Enter the name of the snapshot in the **Snapshot name** box.

RDS > Databases > Take snapshot

Take DB snapshot

Settings
To take a snapshot of this DB instance you must provide a name for the snapshot.

DB instance
The unique key that identifies a DB instance. This parameter isn't case-sensitive.

database-2

Snapshot name
The identifier for the DB snapshot.

Cancel **Take snapshot**

6. Choose **Take snapshot**.

The **Snapshots** page appears, with the new DB snapshot's status shown as *Creating*. After its status is *Available*, you can see its creation time.

AWS CLI

When you create a DB snapshot using the AWS CLI, you need to identify which DB instance you are going to back up, and then give your DB snapshot a name so you can restore from it later. You can do this by using the AWS CLI [create-db-snapshot](#) command with the following parameters:

- `--db-instance-identifier`
- `--db-snapshot-identifier`

In this example, you create a DB snapshot called `mydbsnapshot` for a DB instance called `mydbinstance`.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-snapshot \
  --db-instance-identifier mydbinstance \
  --db-snapshot-identifier mydbsnapshot
```

For Windows:

```
aws rds create-db-snapshot ^
  --db-instance-identifier mydbinstance ^
  --db-snapshot-identifier mydbsnapshot
```

RDS API

When you create a DB snapshot using the Amazon RDS API, you need to identify which DB instance you are going to back up, and then give your DB snapshot a name so you can restore from it later. You can do this by using the Amazon RDS API [CreateDBSnapshot](#) command with the following parameters:

- `DBInstanceIdentifier`
- `DBSnapshotIdentifier`

Creating a Multi-AZ DB cluster snapshot

When you create a Multi-AZ DB cluster snapshot, make sure to identify which Multi-AZ DB cluster you are going to back up, and then give your DB cluster snapshot a name so you can restore from it later.

You can create a Multi-AZ DB cluster snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To create a DB cluster snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. In the list, choose the Multi-AZ DB cluster for which you want to take a snapshot.
4. For **Actions**, choose **Take snapshot**.

The **Take DB snapshot** window appears.

5. For **Snapshot name**, enter the name of the snapshot.
6. Choose **Take snapshot**.

The **Snapshots** page appears, with the new Multi-AZ DB cluster snapshot's status shown as **Creating**. After its status is **Available**, you can see its creation time.

AWS CLI

You can create a Multi-AZ DB cluster snapshot by using the AWS CLI `create-db-cluster-snapshot` command with the following options:

- `--db-cluster-identifier`
- `--db-cluster-snapshot-identifier`

In this example, you create a Multi-AZ DB cluster snapshot called `mymultiazdbclustersnapshot` for a DB cluster called `mymultiazdbcluster`.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-cluster-snapshot \
  --db-cluster-identifier mymultiazdbcluster \
  --db-cluster-snapshot-identifier mymultiazdbclustersnapshot
```

For Windows:

```
aws rds create-db-cluster-snapshot ^
  --db-cluster-identifier mymultiazdbcluster ^
  --db-cluster-snapshot-identifier mymultiazdbclustersnapshot
```

RDS API

You can create a Multi-AZ DB cluster snapshot by using the Amazon RDS API `CreateDBClusterSnapshot` operation with the following parameters:

- **DBClusterIdentifier**
- **DBClusterSnapshotIdentifier**

Restoring from a DB snapshot

Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. You can create a new DB instance by restoring from a DB snapshot. You provide the name of the DB snapshot to restore from, and then provide a name for the new DB instance that is created from the restore. You can't restore from a DB snapshot to an existing DB instance; a new DB instance is created when you restore.

You can use the restored DB instance as soon as its status is available. The DB instance continues to load data in the background. This is known as *lazy loading*.

If you access data that hasn't been loaded yet, the DB instance immediately downloads the requested data from Amazon S3, and then continues loading the rest of the data in the background. For more information, see [Amazon EBS snapshots](#).

To help mitigate the effects of lazy loading on tables to which you require quick access, you can perform operations that involve full-table scans, such as `SELECT *`. This allows Amazon RDS to download all of the backed-up table data from S3.

You can restore a DB instance and use a different storage type than the source DB snapshot. In this case, the restoration process is slower because of the additional work required to migrate the data to the new storage type. If you restore to or from magnetic storage, the migration process is the slowest. That's because magnetic storage doesn't have the IOPS capability of Provisioned IOPS or General Purpose (SSD) storage.

You can use AWS CloudFormation to restore a DB instance from a DB instance snapshot. For more information, see [AWS::RDS::DBInstance](#) in the *AWS CloudFormation User Guide*.

Note

You can't restore a DB instance from a DB snapshot that is both shared and encrypted. Instead, you can make a copy of the DB snapshot and restore the DB instance from the copy. For more information, see [Copying a DB snapshot \(p. 458\)](#).

Parameter group considerations

We recommend that you retain the DB parameter group for any DB snapshots you create, so that you can associate your restored DB instance with the correct parameter group.

The default DB parameter group is associated with the restored instance, unless you choose a different one. No custom parameter settings are available in the default parameter group.

You can specify the parameter group when you restore the DB instance.

For more information about DB parameter groups, see [Working with parameter groups \(p. 289\)](#).

Security group considerations

When you restore a DB instance, the default virtual private cloud (VPC), DB subnet group, and VPC security group are associated with the restored instance, unless you choose different ones.

- If you're using the Amazon RDS console, you can specify a custom VPC security group to associate with the instance or create a new VPC security group.
- If you're using the AWS CLI, you can specify a custom VPC security group to associate with the instance by including the `--vpc-security-group-ids` option in the `restore-db-instance-from-db-snapshot` command.

- If you're using the Amazon RDS API, you can include the `VpcSecurityGroupIds.VpcSecurityGroupId.N` parameter in the `RestoreDBInstanceFromDBSnapshot` action.

As soon as the restore is complete and your new DB instance is available, you can also change the VPC settings by modifying the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Option group considerations

When you restore a DB instance, the default DB option group is associated with the restored DB instance in most cases.

The exception is when the source DB instance is associated with an option group that contains a persistent or permanent option. For example, if the source DB instance uses Oracle Transparent Data Encryption (TDE), the restored DB instance must use an option group that has the TDE option.

If you restore a DB instance into a different VPC, you must do one of the following to assign a DB option group:

- Assign the default option group for that VPC group to the instance.
- Assign another option group that is linked to that VPC.
- Create a new option group and assign it to the DB instance. With persistent or permanent options, such as Oracle TDE, you must create a new option group that includes the persistent or permanent option.

For more information about DB option groups, see [Working with option groups \(p. 273\)](#).

Resource tagging considerations

When you restore a DB instance from a DB snapshot, RDS checks whether you specify new tags. If yes, the new tags are added to the restored DB instance. If there are no new tags, RDS looks for the tags from the source DB instance for the DB snapshot, and then adds those tags to the restored DB instance.

For more information, see [Copying tags to DB instance snapshots \(p. 396\)](#).

Microsoft SQL Server considerations

When you restore an RDS for Microsoft SQL Server DB snapshot to a new instance, you can always restore to the same edition as your snapshot. In some cases, you can also change the edition of the DB instance. The following limitations apply when you change editions:

- The DB snapshot must have enough storage allocated for the new edition.
- Only the following edition changes are supported:
 - From Standard Edition to Enterprise Edition
 - From Web Edition to Standard Edition or Enterprise Edition
 - From Express Edition to Web Edition, Standard Edition, or Enterprise Edition

If you want to change from one edition to a new edition that isn't supported by restoring a snapshot, you can try using the native backup and restore feature. SQL Server verifies whether your database is compatible with the new edition based on what SQL Server features you have enabled on the database. For more information, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Oracle Database considerations

If you use Oracle GoldenGate, always retain the parameter group with the compatible parameter. When you restore a DB instance from a DB snapshot, specify a parameter group that has a matching or greater compatible value.

If you restore a snapshot of a CDB instance, you can change the PDB name. You can't change the CDB name, which is always RDSCDB. This CDB name is the same for all RDS instances that use a single-tenant architecture. For more information, see [Snapshots in a single-tenant architecture \(p. 1482\)](#).

Before you restore a DB snapshot, you can upgrade it to a later release. For more information, see [Upgrading an Oracle DB snapshot \(p. 1764\)](#).

Restoring from a snapshot

You can restore a DB instance from a DB snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore a DB instancefrom a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to restore from.
4. For **Actions**, choose **Restore snapshot**.
5. On the **Restore snapshot** page, for **DB instance identifier**, enter the name for your restored DB instance.
6. Specify other settings.

For information about each setting, see [Settings for DB instances \(p. 237\)](#).

7. Choose **Restore DB instance**.

AWS CLI

To restore a DB instance from a DB snapshot, use the AWS CLI command `restore-db-instance-from-db-snapshot`.

In this example, you restore from a previously created DB snapshot named `mydbsnapshot`. You restore to a new DB instance named `mynewdbinstance`.

You can specify other settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-from-db-snapshot \
--db-instance-identifier mynewdbinstance \
--db-snapshot-identifier mydbsnapshot
```

For Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
--db-instance-identifier mynewdbinstance ^
--db-snapshot-identifier mydbsnapshot
```

This command returns output similar to the following:

```
DBINSTANCE mynewdbinstance db.t3.small MySQL 50 sa creating 3 n
8.0.28 general-public-license
```

RDS API

To restore a DB instance from a DB snapshot, call the Amazon RDS API function [RestoreDBInstanceFromDBSnapshot](#) with the following parameters:

- **DBInstanceIdentifier**
- **DBSnapshotIdentifier**

Restoring from a snapshot to a Multi-AZ DB cluster

You can restore a snapshot to a Multi-AZ DB cluster using the AWS Management Console, the AWS CLI, or the RDS API. You can restore each of these types of snapshots to a Multi-AZ DB cluster:

- A snapshot of a single-AZ deployment
- A snapshot of a Multi-AZ DB instance deployment with a single DB instance
- A snapshot of a Multi-AZ DB cluster

Tip

You can migrate a single-AZ deployment or a Multi-AZ DB instance deployment to a Multi-AZ DB cluster deployment by restoring a snapshot.

Console

To restore a snapshot to a Multi-AZ DB cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the snapshot that you want to restore from.
4. For **Actions**, choose **Restore snapshot**.
5. On the **Restore snapshot** page, in **Availability and durability**, choose **Multi-AZ DB cluster**.

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB cluster
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance
Creates a single DB instance with no standby DB instances.

6. In **DB instance class**, choose a DB instance class.
Currently, Multi-AZ DB clusters only support db.m6gd and db.r6gd DB instance classes. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).
7. For **DB cluster identifier**, enter the name for your restored Multi-AZ DB cluster.
8. For the remaining sections, specify your DB cluster settings. For information about each setting, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).
9. Choose **Restore DB cluster**.

AWS CLI

To restore a snapshot to a Multi-AZ DB cluster, use the AWS CLI command [restore-db-cluster-from-snapshot](#).

In the following example, you restore from a previously created snapshot named `mysnapshot`. You restore to a new Multi-AZ DB cluster named `mynewmultiazdbcluster`. You also specify the DB instance class used by the DB instances in the Multi-AZ DB cluster. Specify either `mysql` or `postgres` for the DB engine.

For the `--snapshot-identifier` option, you can use either the name or the Amazon Resource Name (ARN) to specify a DB cluster snapshot. However, you can use only the ARN to specify a DB snapshot.

Currently, Multi-AZ DB clusters only support `db.m6gd` and `db.r6gd` DB instance classes. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-cluster-from-snapshot \
--db-cluster-identifier mynewmultiazdbcluster \
--snapshot-identifier mysnapshot \
--engine mysql|postgres \
--db-cluster-instance-class db.r6gd.xlarge
```

For Windows:

```
aws rds restore-db-cluster-from-snapshot ^
--db-cluster-identifier mynewmultiazdbcluster ^
--snapshot-identifier mysnapshot ^
--engine mysql|postgres ^
--db-cluster-instance-class db.r6gd.xlarge
```

After the DB cluster has been restored, make sure to add the Multi-AZ DB cluster to the security group used by the DB cluster or DB instance used to create the snapshot. Doing so provides the same functionality as that of the previous DB cluster or DB instance.

RDS API

To restore a snapshot to a Multi-AZ DB cluster, call the RDS API operation [RestoreDBClusterFromSnapshot](#) with the following parameters:

- `DBClusterIdentifier`
- `SnapshotIdentifier`
- `Engine`

You can also specify other optional parameters.

After the DB cluster has been restored, make sure to add the Multi-AZ DB cluster to the security group used by the DB cluster or DB instance used to create the snapshot. Doing so provides the same functionality as that of the previous DB cluster or DB instance.

Copying a DB snapshot

With Amazon RDS, you can copy automated backups or manual DB snapshots. After you copy a snapshot, the copy is a manual snapshot. You can make multiple copies of an automated backup or manual snapshot, but each copy must have a unique identifier.

You can copy a snapshot within the same AWS Region, you can copy a snapshot across AWS Regions, and you can copy shared snapshots.

Limitations

The following are some limitations when you copy snapshots:

- You can't copy a snapshot to or from the China (Beijing) Region or the China (Ningxia) Region.
- You can copy a snapshot between AWS GovCloud (US-East) and AWS GovCloud (US-West). However, you can't copy a snapshot between these GovCloud (US) Regions and Regions that aren't GovCloud (US) Regions.
- If you delete a source snapshot before the target snapshot becomes available, the snapshot copy might fail. Verify that the target snapshot has a status of AVAILABLE before you delete a source snapshot.
- You can have up to 20 snapshot copy requests in progress to a single destination Region per account.
- When you request multiple snapshot copies for the same source DB instance, they're queued internally. The copies requested later won't start until the previous snapshot copies are completed. For more information, see [Why is my EC2 AMI or EBS snapshot creation slow?](#) in the AWS Knowledge Center.
- Depending on the AWS Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete. In some cases, there might be a large number of cross-Region snapshot copy requests from a given source Region. In such cases, Amazon RDS might put new cross-Region copy requests from that source Region into a queue until some in-progress copies complete. No progress information is displayed about copy requests while they are in the queue. Progress information is displayed when the copy starts.

Snapshot retention

Amazon RDS deletes automated backups in several situations:

- At the end of their retention period.
- When you disable automated backups for a DB instance.
- When you delete a DB instance.

If you want to keep an automated backup for a longer period, copy it to create a manual snapshot, which is retained until you delete it. Amazon RDS storage costs might apply to manual snapshots if they exceed your default storage space.

For more information about backup storage costs, see [Amazon RDS pricing](#).

Copying shared snapshots

You can copy snapshots shared to you by other AWS accounts. In some cases, you might copy an encrypted snapshot that has been shared from another AWS account. In these cases, you must have access to the AWS KMS key that was used to encrypt the snapshot.

You can copy a shared DB snapshot across AWS Regions if the snapshot is unencrypted. However, if the shared DB snapshot is encrypted, you can only copy it in the same Region.

Note

Copying shared incremental snapshots in the same AWS Region is supported when they're unencrypted, or encrypted using the same KMS key as the initial full snapshot. If you use a different KMS key to encrypt subsequent snapshots when copying them, those shared snapshots are full snapshots. For more information, see [Incremental snapshot copying \(p. 459\)](#).

Handling encryption

You can copy a snapshot that has been encrypted using a KMS key. If you copy an encrypted snapshot, the copy of the snapshot must also be encrypted. If you copy an encrypted snapshot within the same AWS Region, you can encrypt the copy with the same KMS key as the original snapshot. Or you can specify a different KMS key.

If you copy an encrypted snapshot across Regions, you must specify a KMS key valid in the destination AWS Region. It can be a Region-specific KMS key, or a multi-Region key. For more information on multi-Region KMS keys, see [Using multi-Region keys in AWS KMS](#).

The source snapshot remains encrypted throughout the copy process. For more information, see [Limitations of Amazon RDS encrypted DB instances \(p. 2003\)](#).

You can also encrypt a copy of an unencrypted snapshot. This way, you can quickly add encryption to a previously unencrypted DB instance. To do this, you create a snapshot of your DB instance when you are ready to encrypt it. You then create a copy of that snapshot and specify a KMS key to encrypt that snapshot copy. You can then restore an encrypted DB instance from the encrypted snapshot.

Incremental snapshot copying

An *incremental* snapshot contains only the data that has changed after the most recent snapshot of the same DB instance. Incremental snapshot copying is faster and results in lower storage costs than full snapshot copying.

Note

When you copy a source snapshot that is a snapshot copy itself, the new copy isn't incremental. This is because the source snapshot copy doesn't include the required metadata for incremental copies.

Whether a snapshot copy is incremental is determined by the most recently completed snapshot copy. If the most recent snapshot copy was deleted, the next copy is a full copy, not an incremental copy.

If a copy is still pending when you start another copy, the second copy doesn't start until the first copy finishes.

When you copy a snapshot across AWS accounts, the copy is an incremental copy if the following conditions are met:

- A different snapshot of the same source DB instance was previously copied to the destination account.
- The most recent snapshot copy still exists in the destination account.
- All copies of the snapshot in the destination account are either unencrypted, or were encrypted using the same KMS key.

The following examples illustrate the difference between full and incremental snapshots. They apply to both shared and unshared snapshots.

Snapshot	Encryption key	Full or incremental
S1	K1	Full

Snapshot	Encryption key	Full or incremental
S2	K1	Incremental of S1
S3	K1	Incremental of S2
S4	K1	Incremental of S3
Copy of S1 (S1C)	K2	Full
Copy of S2 (S2C)	K3	Full
Copy of S3 (S3C)	K3	Incremental of S2C
Copy of S4 (S4C)	K3	Incremental of S3C
Copy 2 of S4 (S4C2)	K4	Full

Note

In these examples, snapshots S2, S3, and S4 are incremental only if the previous snapshot still exists.

The same applies to copies. Snapshot copies S3C and S4C are incremental only if the previous copy still exists.

For information on copying incremental snapshots across AWS Regions, see [Full and incremental copies \(p. 463\)](#).

Cross-Region snapshot copying

You can copy DB snapshots across AWS Regions. However, there are certain constraints and considerations for cross-Region snapshot copying.

Requesting a cross-Region DB snapshot copy

To communicate with the source Region to request a cross-Region DB snapshot copy, the requester (IAM role or IAM user) must have access to the source DB snapshot and the source Region.

Certain conditions in the requester's IAM policy can cause the request to fail. The following examples assume that you're copying the DB snapshot from US East (Ohio) to US East (N. Virginia). These examples show conditions in the requester's IAM policy that cause the request to fail:

- The requester's policy has a condition for `aws:RequestedRegion`.

```

...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": "us-east-1"
    }
}
}
```

The request fails because the policy doesn't allow access to the source Region. For a successful request, specify both the source and destination Regions.

```

...
"Effect": "Allow",
```

```
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2"
        ]
    }
}
```

- The requester's policy doesn't allow access to the source DB snapshot.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "arn:aws:rds:us-east-1:123456789012:snapshot:target-snapshot"
...
```

For a successful request, specify both the source and target snapshots.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": [
    "arn:aws:rds:us-east-1:123456789012:snapshot:target-snapshot",
    "arn:aws:rds:us-east-2:123456789012:snapshot:source-snapshot"
]
...
```

- The requester's policy denies aws:ViaAWSService.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "Bool": {"aws:ViaAWSService": "false"}
}
```

Communication with the source Region is made by RDS on the requester's behalf. For a successful request, don't deny calls made by AWS services.

- The requester's policy has a condition for aws:SourceVpc or aws:SourceVpce.

These requests might fail because when RDS makes the call to the remote Region, it isn't from the specified VPC or VPC endpoint.

If you need to use one of the previous conditions that would cause a request to fail, you can include a second statement with aws:CalledVia in your policy to make the request succeed. For example, you can use aws:CalledVia with aws:SourceVpce as shown here:

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "Condition" : {
        "ForAnyValue:StringEquals" : {
            "aws:SourceVpce": "vpce-1a2b3c4d"
        }
    }
}
```

```
        },
    },
{
    "Effect": "Allow",
    "Action": [
        "rds:CopyDBSnapshot"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "rds.amazonaws.com"
            ]
        }
    }
}
```

For more information, see [Policies and permissions in IAM](#) in the *IAM User Guide*.

Authorizing the snapshot copy

After a cross-Region DB snapshot copy request returns success, RDS starts the copy in the background. An authorization for RDS to access the source snapshot is created. This authorization links the source DB snapshot to the target DB snapshot, and allows RDS to copy only to the specified target snapshot.

The authorization is verified by RDS using the `rds:CrossRegionCommunication` permission in the service-linked IAM role. If the copy is authorized, RDS communicates with the source Region and completes the copy.

RDS doesn't have access to DB snapshots that weren't authorized previously by a `CopyDBSnapshot` request. The authorization is revoked when copying completes.

RDS uses the service-linked role to verify the authorization in the source Region. If you delete the service-linked role during the copy process, the copy fails.

For more information, see [Using service-linked roles](#) in the *IAM User Guide*.

Using AWS Security Token Service credentials

Session tokens from the global AWS Security Token Service (AWS STS) endpoint are valid only in AWS Regions that are enabled by default (commercial Regions). If you use credentials from the `assumeRole` API operation in AWS STS, use the regional endpoint if the source Region is an opt-in Region. Otherwise, the request fails. This happens because your credentials must be valid in both Regions, which is true for opt-in Regions only when the regional AWS STS endpoint is used.

To use the global endpoint, make sure that it's enabled for both Regions in the operations. Set the global endpoint to `Valid in all AWS Regions` in the AWS STS account settings.

The same rule applies to credentials in the `presigned URL` parameter.

For more information, see [Managing AWS STS in an AWS Region](#) in the *IAM User Guide*.

Latency and multiple copy requests

Depending on the AWS Regions involved and the amount of data to be copied, a cross-Region snapshot copy can take hours to complete.

In some cases, there might be a large number of cross-Region snapshot copy requests from a given source AWS Region. In such cases, Amazon RDS might put new cross-Region copy requests from that

source AWS Region into a queue until some in-progress copies complete. No progress information is displayed about copy requests while they are in the queue. Progress information is displayed when the copying starts.

Full and incremental copies

When you copy a snapshot to a different AWS Region from the source snapshot, the first copy is a full snapshot copy, even if you copy an incremental snapshot. A full snapshot copy contains all of the data and metadata required to restore the DB instance. After the first snapshot copy, you can copy incremental snapshots of the same DB instance to the same destination Region within the same AWS account. For more information on incremental snapshots, see [Incremental snapshot copying \(p. 459\)](#).

Incremental snapshot copying across AWS Regions is supported for both unencrypted and encrypted snapshots.

When you copy a snapshot across AWS Regions, the copy is an incremental copy if the following conditions are met:

- The snapshot was previously copied to the destination Region.
- The most recent snapshot copy still exists in the destination Region.
- All copies of the snapshot in the destination Region are either unencrypted, or were encrypted using the same KMS key.

Option group considerations

Option groups are specific to the AWS Region that they are created in, and you can't use an option group from one AWS Region in another AWS Region.

When you copy a snapshot across Regions, you can specify a new option group for the snapshot. We recommend that you prepare the new option group before you copy the snapshot. In the destination AWS Region, create an option group with the same settings as the original DB instance. If one already exists in the new AWS Region, you can use that one.

In some cases, you might copy a snapshot and not specify a new option group for the snapshot. In these cases, when you restore the snapshot the DB instance gets the default option group. To give the new DB instance the same options as the original, do the following:

1. In the destination AWS Region, create an option group with the same settings as the original DB instance. If one already exists in the new AWS Region, you can use that one.
2. After you restore the snapshot in the destination AWS Region, modify the new DB instance and add the new or existing option group from the previous step.

Parameter group considerations

When you copy a snapshot across Regions, the copy doesn't include the parameter group used by the original DB instance. When you restore a snapshot to create a new DB instance, that DB instance gets the default parameter group for the AWS Region it is created in. To give the new DB instance the same parameters as the original, do the following:

1. In the destination AWS Region, create a DB parameter group with the same settings as the original DB instance. If one already exists in the new AWS Region, you can use that one.
2. After you restore the snapshot in the destination AWS Region, modify the new DB instance and add the new or existing parameter group from the previous step.

Copying a DB snapshot

Use the procedures in this topic to copy a DB snapshot. For an overview of copying a snapshot, see [Copying a DB snapshot \(p. 458\)](#)

For each AWS account, you can copy up to five DB snapshots at a time from one AWS Region to another. If you copy a DB snapshot to another AWS Region, you create a manual DB snapshot that is retained in that AWS Region. Copying a DB snapshot out of the source AWS Region incurs Amazon RDS data transfer charges.

For more information about data transfer pricing, see [Amazon RDS pricing](#).

After the DB snapshot copy has been created in the new AWS Region, the DB snapshot copy behaves the same as all other DB snapshots in that AWS Region.

You can copy a DB snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

The following procedure copies an encrypted or unencrypted DB snapshot, in the same AWS Region or across Regions, by using the AWS Management Console.

To copy a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Select the DB snapshot that you want to copy.
4. For **Actions**, choose **Copy snapshot**.

The **Copy snapshot** page appears.

RDS > Snapshots > Copy snapshot

Copy snapshot

Settings

Source DB Snapshot
DB Snapshot Identifier for the snapshot being copied.
db1-snapshot

Destination Region [Info](#)
US West (Oregon)

New DB Snapshot Identifier
DB Snapshot Identifier for the new snapshot

Target Option Group (Optional)
No preference

Copy Tags [Info](#)

i Please note that depending on the amount of data to be copied and the Region you choose, this operation could take several hours to complete and the display on the progress bar could be delayed until setup is complete.

Encryption

Encryption [Info](#)
 Enable Encryption
Choose to encrypt the copy of the source DB snapshot. Master key IDs and aliases appear in the list after they have been created using KMS. You cannot remove encryption from an encrypted DB snapshot.

Master key [Info](#)
(default) aws/rds

Account

KMS key ID

Cancel **Copy snapshot**

5. (Optional) To copy the DB snapshot to a different AWS Region, for **Destination Region**, choose the new AWS Region.

Note

The destination AWS Region must have the same database engine version available as the source AWS Region.

6. For **New DB Snapshot Identifier**, type the name of the DB snapshot copy.

You can make multiple copies of an automated backup or manual snapshot, but each copy must have a unique identifier.

7. (Optional) For **Target Option Group**, choose a new option group.

Specify this option if you are copying a snapshot from one AWS Region to another, and your DB instance uses a nondefault option group.

If your source DB instance uses Transparent Data Encryption for Oracle or Microsoft SQL Server, you must specify this option when copying across Regions. For more information, see [Option group considerations \(p. 463\)](#).

8. (Optional) Select **Copy Tags** to copy tags and values from the snapshot to the copy of the snapshot.
9. (Optional) For **Encryption**, do the following:

- a. Choose **Enable Encryption** if the DB snapshot isn't encrypted but you want to encrypt the copy.

Note

If the DB snapshot is encrypted, you must encrypt the copy, so the check box is already selected.

- b. For **AWS KMS key**, specify the KMS key identifier to use to encrypt the DB snapshot copy.

10. Choose **Copy snapshot**.

AWS CLI

You can copy a DB snapshot by using the AWS CLI command `copy-db-snapshot`. If you are copying the snapshot to a new AWS Region, run the command in the new AWS Region.

The following options are used to copy a DB snapshot. Not all options are required for all scenarios. Use the descriptions and the examples that follow to determine which options to use.

- `--source-db-snapshot-identifier` – The identifier for the source DB snapshot.
 - If the source snapshot is in the same AWS Region as the copy, specify a valid DB snapshot identifier. For example, `rds:mysql-instance1-snapshot-20130805`.
 - If the source snapshot is in a different AWS Region than the copy, specify a valid DB snapshot ARN. For example, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
 - If you are copying from a shared manual DB snapshot, this parameter must be the Amazon Resource Name (ARN) of the shared DB snapshot.
 - If you are copying an encrypted snapshot this parameter must be in the ARN format for the source AWS Region, and must match the `SourceDBSnapshotIdentifier` in the `PreSignedUrl` parameter.
- `--target-db-snapshot-identifier` – The identifier for the new copy of the encrypted DB snapshot.
- `--copy-tags` – Include the `copy tags` option to copy tags and values from the snapshot to the copy of the snapshot.
- `--option-group-name` – The option group to associate with the copy of the snapshot.

Specify this option if you are copying a snapshot from one AWS Region to another, and your DB instance uses a non-default option group.

If your source DB instance uses Transparent Data Encryption for Oracle or Microsoft SQL Server, you must specify this option when copying across Regions. For more information, see [Option group considerations \(p. 463\)](#).

- `--kms-key-id` – The KMS key identifier for an encrypted DB snapshot. The KMS key identifier is the Amazon Resource Name (ARN), key identifier, or key alias for the KMS key.
 - If you copy an encrypted DB snapshot from your AWS account, you can specify a value for this parameter to encrypt the copy with a new KMS key. If you don't specify a value for this parameter, then the copy of the DB snapshot is encrypted with the same KMS key as the source DB snapshot.
 - If you copy an encrypted DB snapshot that is shared from another AWS account, then you must specify a value for this parameter.
 - If you specify this parameter when you copy an unencrypted snapshot, the copy is encrypted.
 - If you copy an encrypted snapshot to a different AWS Region, then you must specify a KMS key for the destination AWS Region. KMS keys are specific to the AWS Region that they are created in, and you cannot use encryption keys from one AWS Region in another AWS Region.

Example from unencrypted, to the same Region

The following code creates a copy of a snapshot, with the new name `mydbsnapshotcopy`, in the same AWS Region as the source snapshot. When the copy is made, all tags on the original snapshot are copied to the snapshot copy.

For Linux, macOS, or Unix:

```
aws rds copy-db-snapshot \
  --source-db-snapshot-identifier mysql-instance1-snapshot-20130805 \
  --target-db-snapshot-identifier mydbsnapshotcopy \
  --copy-tags
```

For Windows:

```
aws rds copy-db-snapshot ^
  --source-db-snapshot-identifier mysql-instance1-snapshot-20130805 ^
  --target-db-snapshot-identifier mydbsnapshotcopy ^
  --copy-tags
```

Example from unencrypted, across Regions

The following code creates a copy of a snapshot, with the new name `mydbsnapshotcopy`, in the AWS Region in which the command is run.

For Linux, macOS, or Unix:

```
aws rds copy-db-snapshot \
  --source-db-snapshot-identifier arn:aws:rds:us-east-1:123456789012:snapshot:mysql-
instance1-snapshot-20130805 \
  --target-db-snapshot-identifier mydbsnapshotcopy
```

For Windows:

```
aws rds copy-db-snapshot ^
  --source-db-snapshot-identifier arn:aws:rds:us-east-1:123456789012:snapshot:mysql-
instance1-snapshot-20130805 ^
  --target-db-snapshot-identifier mydbsnapshotcopy
```

Example from encrypted, across Regions

The following code example copies an encrypted DB snapshot from the US West (Oregon) Region in the US East (N. Virginia) Region. Run the command in the destination (us-east-1) Region.

For Linux, macOS, or Unix:

```
aws rds copy-db-snapshot \
--source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-
instance1-snapshot-20161115 \
--target-db-snapshot-identifier mydbsnapshotcopy \
--kms-key-id my-us-east-1-key \
--option-group-name custom-option-group-name
```

For Windows:

```
aws rds copy-db-snapshot ^
--source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-
instance1-snapshot-20161115 ^
--target-db-snapshot-identifier mydbsnapshotcopy ^
--kms-key-id my-us-east-1-key ^
--option-group-name custom-option-group-name
```

The `--source-region` parameter is required when you're copying an encrypted snapshot between the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. For `--source-region`, specify the AWS Region of the source DB instance.

If `--source-region` isn't specified, specify a `--pre-signed-url` value. A *presigned URL* is a URL that contains a Signature Version 4 signed request for the `copy-db-snapshot` command that's called in the source AWS Region. To learn more about the `pre-signed-url` option, see [copy-db-snapshot](#) in the [AWS CLI Command Reference](#).

RDS API

You can copy a DB snapshot by using the Amazon RDS API operation [CopyDBSnapshot](#). If you are copying the snapshot to a new AWS Region, perform the action in the new AWS Region.

The following parameters are used to copy a DB snapshot. Not all parameters are required for all scenarios. Use the descriptions and the examples that follow to determine which parameters to use.

- `SourceDBSnapshotIdentifier` – The identifier for the source DB snapshot.
 - If the source snapshot is in the same AWS Region as the copy, specify a valid DB snapshot identifier. For example, `rds:mysql-instance1-snapshot-20130805`.
 - If the source snapshot is in a different AWS Region than the copy, specify a valid DB snapshot ARN. For example, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
 - If you are copying from a shared manual DB snapshot, this parameter must be the Amazon Resource Name (ARN) of the shared DB snapshot.
 - If you are copying an encrypted snapshot this parameter must be in the ARN format for the source AWS Region, and must match the `SourceDBSnapshotIdentifier` in the `PreSignedUrl` parameter.
- `TargetDBSnapshotIdentifier` – The identifier for the new copy of the encrypted DB snapshot.
- `CopyTags` – Set this parameter to `true` to copy tags and values from the snapshot to the copy of the snapshot. The default is `false`.
- `OptionGroupName` – The option group to associate with the copy of the snapshot.

Specify this parameter if you are copying a snapshot from one AWS Region to another, and your DB instance uses a non-default option group.

If your source DB instance uses Transparent Data Encryption for Oracle or Microsoft SQL Server, you must specify this parameter when copying across Regions. For more information, see [Option group considerations \(p. 463\)](#).

- **KmsKeyId** – The KMS key identifier for an encrypted DB snapshot. The KMS key identifier is the Amazon Resource Name (ARN), key identifier, or key alias for the KMS key.
 - If you copy an encrypted DB snapshot from your AWS account, you can specify a value for this parameter to encrypt the copy with a new KMS key. If you don't specify a value for this parameter, then the copy of the DB snapshot is encrypted with the same KMS key as the source DB snapshot.
 - If you copy an encrypted DB snapshot that is shared from another AWS account, then you must specify a value for this parameter.
 - If you specify this parameter when you copy an unencrypted snapshot, the copy is encrypted.
 - If you copy an encrypted snapshot to a different AWS Region, then you must specify a KMS key for the destination AWS Region. KMS keys are specific to the AWS Region that they are created in, and you cannot use encryption keys from one AWS Region in another AWS Region.
- **PreSignedUrl** – The URL that contains a Signature Version 4 signed request for the `CopyDBSnapshot` API operation in the source AWS Region that contains the source DB snapshot to copy.

Specify this parameter when you copy an encrypted DB snapshot from another AWS Region by using the Amazon RDS API. You can specify the source Region option instead of this parameter when you copy an encrypted DB snapshot from another AWS Region by using the AWS CLI.

The presigned URL must be a valid request for the `CopyDBSnapshot` API operation that can be run in the source AWS Region containing the encrypted DB snapshot to be copied. The presigned URL request must contain the following parameter values:

- **DestinationRegion** – The AWS Region that the encrypted DB snapshot will be copied to. This AWS Region is the same one where the `CopyDBSnapshot` operation is called that contains this presigned URL.

For example, suppose that you copy an encrypted DB snapshot from the us-west-2 Region to the us-east-1 Region. You then call the `CopyDBSnapshot` operation in the us-east-1 Region and provide a presigned URL that contains a call to the `CopyDBSnapshot` operation in the us-west-2 Region. For this example, the **DestinationRegion** in the presigned URL must be set to the us-east-1 Region.

- **KmsKeyId** – The KMS key identifier for the key to use to encrypt the copy of the DB snapshot in the destination AWS Region. This is the same identifier for both the `CopyDBSnapshot` operation that is called in the destination AWS Region, and the operation contained in the presigned URL.
- **SourceDBSnapshotIdentifier** – The DB snapshot identifier for the encrypted snapshot to be copied. This identifier must be in the Amazon Resource Name (ARN) format for the source AWS Region. For example, if you are copying an encrypted DB snapshot from the us-west-2 Region, then your **SourceDBSnapshotIdentifier** looks like the following example: `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20161115`.

For more information on Signature Version 4 signed requests, see the following:

- [Authenticating requests: Using query parameters \(AWS signature version 4\)](#) in the Amazon Simple Storage Service API Reference
- [Signature version 4 signing process](#) in the AWS General Reference

Example from unencrypted, to the same Region

The following code creates a copy of a snapshot, with the new name `mydbsnapshotcopy`, in the same AWS Region as the source snapshot. When the copy is made, all tags on the original snapshot are copied to the snapshot copy.

```
https://rds.us-west-1.amazonaws.com/  
?Action=CopyDBSnapshot  
&CopyTags=true  
&SignatureMethod=HmacSHA256  
&SignatureVersion=4  
&SourceDBSnapshotIdentifier=mysql-instance1-snapshot-20130805  
&TargetDBSnapshotIdentifier=mydbsnapshotcopy  
&Version=2013-09-09  
&X-Amz-Algorithm=AWS4-HMAC-SHA256  
&X-Amz-Credential=AKIADQKE4SARGYLE/20140429/us-west-1/rds/aws4_request  
&X-Amz-Date=20140429T175351Z  
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date  
&X-Amz-Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Example from unencrypted, across Regions

The following code creates a copy of a snapshot, with the new name mydbsnapshotcopy, in the US West (N. California) Region.

```
https://rds.us-west-1.amazonaws.com/  
?Action=CopyDBSnapshot  
&SignatureMethod=HmacSHA256  
&SignatureVersion=4  
&SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-east-1%3A123456789012%3Asnapshot%3Amysql-  
instance1-snapshot-20130805  
&TargetDBSnapshotIdentifier=mydbsnapshotcopy  
&Version=2013-09-09  
&X-Amz-Algorithm=AWS4-HMAC-SHA256  
&X-Amz-Credential=AKIADQKE4SARGYLE/20140429/us-west-1/rds/aws4_request  
&X-Amz-Date=20140429T175351Z  
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date  
&X-Amz-Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Example from encrypted, across Regions

The following code creates a copy of a snapshot, with the new name mydbsnapshotcopy, in the US East (N. Virginia) Region.

```
https://rds.us-east-1.amazonaws.com/  
?Action=CopyDBSnapshot  
&KmsKeyId=my-us-east-1-key  
&OptionGroupName=custom-option-group-name  
&PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F  
%253FAction%253DCopyDBSnapshot  
%2526DestinationRegion%253Dus-east-1  
%2526KmsKeyId%253Dmy-us-east-1-key  
%2526SourceDBSnapshotIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-  
west-2%25253A123456789012%25253Asnapshot%25253Amysql-instance1-snapshot-20161115  
%2526SignatureMethod%253DHmacSHA256  
%2526SignatureVersion%253D4  
%2526Version%253D2014-10-31  
%2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256  
%2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-west-2%252Frds  
%252Faws4_request  
%2526X-Amz-Date%253D20161117T215409Z  
%2526X-Amz-Expires%253D3600  
%2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-amz-  
content-sha256%253Bx-amz-date  
%2526X-Amz-Signature  
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613  
&SignatureMethod=HmacSHA256  
&SignatureVersion=4
```

```
&SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-west-2%3A123456789012%3Asnapshot
%3Amysql-instance1-snapshot-20161115
&TargetDBSnapshotIdentifier=mydbsnapshotcopy
&Version=2014-10-31
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
&X-Amz-Date=20161117T221704Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=da4f2da66739d2e722c85fcfd225dc27bba7e2b8dbea8d8612434378e52adccf
```

Sharing a DB snapshot

Using Amazon RDS, you can share a manual DB snapshot in the following ways:

- Sharing a manual DB snapshot, whether encrypted or unencrypted, enables authorized AWS accounts to copy the snapshot.
- Sharing an unencrypted manual DB snapshot enables authorized AWS accounts to directly restore a DB instance from the snapshot instead of taking a copy of it and restoring from that. However, you can't restore a DB instance from a DB snapshot that is both shared and encrypted. Instead, you can make a copy of the DB snapshot and restore the DB instance from the copy.

Note

To share an automated DB snapshot, create a manual DB snapshot by copying the automated snapshot, and then share that copy. This process also applies to AWS Backup-generated resources.

For more information on copying a snapshot, see [Copying a DB snapshot \(p. 458\)](#). For more information on restoring a DB instance from a DB snapshot, see [Restoring from a DB snapshot \(p. 452\)](#).

You can share a manual snapshot with up to 20 other AWS accounts.

The following limitations apply when sharing manual snapshots with other AWS accounts:

- When you restore a DB instance from a shared snapshot using the AWS Command Line Interface (AWS CLI) or Amazon RDS API, you must specify the Amazon Resource Name (ARN) of the shared snapshot as the snapshot identifier.
- You can't share a DB snapshot that uses an option group with permanent or persistent options, except for Oracle DB instances that have the Timezone or OLS option (or both).

A *permanent option* can't be removed from an option group. Option groups with persistent options can't be removed from a DB instance once the option group has been assigned to the DB instance.

The following table lists permanent and persistent options and their related DB engines.

Option name	Persistent	Permanent	DB engine
TDE	Yes	No	Microsoft SQL Server Enterprise Edition
TDE	Yes	Yes	Oracle Enterprise Edition
Timezone	Yes	Yes	Oracle Enterprise Edition
			Oracle Standard Edition
			Oracle Standard Edition One
			Oracle Standard Edition Two

For Oracle DB instances, you can copy shared DB snapshots that have the Timezone or OLS option (or both). To do so, specify a target option group that includes these options when you copy the DB snapshot. The OLS option is permanent and persistent only for Oracle DB instances running Oracle version 12.2 or higher. For more information about these options, see [Oracle time zone \(p. 1742\)](#) and [Oracle Label Security \(p. 1703\)](#).

Sharing public snapshots

You can also share an unencrypted manual snapshot as public, which makes the snapshot available to all AWS accounts. Make sure when sharing a snapshot as public that none of your private information is included in the public snapshot.

When a snapshot is shared publicly, it gives all AWS accounts permission both to copy the snapshot and to create DB instances from it.

You aren't billed for the backup storage of public snapshots owned by other accounts. You're billed only for snapshots that you own.

If you copy a public snapshot, you own the copy. You're billed for the backup storage of your snapshot copy. If you create a DB instance from a public snapshot, you're billed for that DB instance. For Amazon RDS pricing information, see the [Amazon RDS product page](#).

You can delete only the public snapshots that you own. To delete a shared or public snapshot, make sure to log into the AWS account that owns the snapshot.

Viewing public snapshots owned by other AWS accounts

You can view public snapshots owned by other accounts in a particular AWS Region on the **Public** tab of the **Snapshots** page in the Amazon RDS console. Your snapshots (those owned by your account) don't appear on this tab.

To view public snapshots

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the **Public** tab.

The public snapshots appear. You can see which account owns a public snapshot in the **Owner** column.

Note

You might have to modify the page preferences, by selecting the gear icon at the upper right of the **Public snapshots** list, to see this column.

Viewing your own public snapshots

You can use the following AWS CLI command (Unix only) to view the public snapshots owned by your AWS account in a particular AWS Region.

```
aws rds describe-db-snapshots --snapshot-type public --include-public | grep account_number
```

The output returned is similar to the following example if you have public snapshots.

```
"DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mysnapshot1",
"DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mysnapshot2",
```

Note

You might see duplicate entries for `DBSnapshotIdentifier` or `SourceDBSnapshotIdentifier`.

Sharing encrypted snapshots

You can share DB snapshots that have been encrypted "at rest" using the AES-256 encryption algorithm, as described in [Encrypting Amazon RDS resources \(p. 2000\)](#). To do this, take the following steps:

1. Share the AWS KMS key that was used to encrypt the snapshot with any accounts that you want to be able to access the snapshot.

You can share KMS keys with another AWS account by adding the other account to the KMS key policy. For details on updating a key policy, see [Key policies](#) in the *AWS KMS Developer Guide*. For an example of creating a key policy, see [Allowing access to an AWS KMS key \(p. 474\)](#) later in this topic.

2. Use the AWS Management Console, AWS CLI, or Amazon RDS API to share the encrypted snapshot with the other accounts.

These restrictions apply to sharing encrypted snapshots:

- You can't share encrypted snapshots as public.
- You can't share Oracle or Microsoft SQL Server snapshots that are encrypted using Transparent Data Encryption (TDE).
- You can't share a snapshot that has been encrypted using the default KMS key of the AWS account that shared the snapshot.

Allowing access to an AWS KMS key

For another AWS account to copy an encrypted DB snapshot shared from your account, the account that you share your snapshot with must have access to the AWS KMS key that encrypted the snapshot.

To allow another AWS account access to a KMS key, update the key policy for the KMS key. You update it with the Amazon Resource Name (ARN) of the AWS account that you are sharing to as `Principal` in the KMS key policy. Then you allow the `kms:CreateGrant` action.

After you have given an AWS account access to your KMS key, to copy your encrypted snapshot that AWS account must create an AWS Identity and Access Management (IAM) role or user if it doesn't already have one. In addition, that AWS account must also attach an IAM policy to that IAM role or user that allows the role or user to copy an encrypted DB snapshot using your KMS key. The account must be an IAM user and can't be a root AWS account identity due to AWS KMS security restrictions.

In the following key policy example, user 111122223333 is the owner of the KMS key, and user 444455556666 is the account that the key is being shared with. This updated key policy gives the AWS account access to the KMS key by including the ARN for the root AWS account identity for user 444455556666 as a `Principal` for the policy, and by allowing the `kms:CreateGrant` action.

```
{  
    "Id": "key-policy-1",  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Allow use of the key",  
            "Effect": "Allow",  
            "Principal": {"AWS": [  
                "arn:aws:iam::111122223333:user/KeyUser",  
                "arn:aws:iam::444455556666:root"  
            ]},  
            "Action": [  
                "kms:CreateGrant",  
                "kms:Decrypt",  
                "kms:DescribeKey",  
                "kms:Encrypt",  
                "kms:GenerateDataKey",  
                "kms:GenerateDataKeyWithoutPlaintext",  
                "kms:ListAliases",  
                "kms:ListKeys",  
                "kms:ReEncryptFrom",  
                "kms:ReEncryptTo",  
                "kms:UpdateKeyDescription",  
                "kms:UpdateKeyPolicy"  
            ]  
        }  
    ]  
}
```

```

        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/KeyUser",
        "arn:aws:iam::444455556666:root"
    ]},
    "Action": [
        "kms:CreateGrant",
        "kms>ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
]
}

```

Creating an IAM policy to enable copying of the encrypted snapshot

Once the external AWS account has access to your KMS key, the owner of that AWS account can create a policy that allows an IAM user created for that account to copy an encrypted snapshot encrypted with that KMS key.

The following example shows a policy that can be attached to an IAM user for AWS account 444455556666 that enables the IAM user to copy a shared snapshot from AWS account 111122223333 that has been encrypted with the KMS key c989c1dd-a3f2-4a5d-8d96-e793d082ab26 in the us-west-2 region.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms>CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource": ["arn:aws:kms:us-west-2:111122223333:key/c989c1dd-a3f2-4a5d-8d96-e793d082ab26"]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms>CreateGrant",
                "kms>ListGrants",
                "kms:RevokeGrant"
            ]
        }
    ]
}

```

```
        ],
        "Resource": ["arn:aws:kms:us-west-2:111122223333:key/c989c1dd-a3f2-4a5d-8d96-
e793d082ab26"],
        "Condition": {
            "Bool": {
                "kms:GrantIsForAWSResource": true
            }
        }
    ]
}
```

For details on updating a key policy, see [Key policies in the AWS KMS Developer Guide](#).

Sharing a snapshot

You can share a DB snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

Console

Using the Amazon RDS console, you can share a manual DB snapshot with up to 20 AWS accounts. You can also use the console to stop sharing a manual snapshot with one or more accounts.

To share a manual DB snapshot by using the Amazon RDS console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Select the manual snapshot that you want to share.
4. For **Actions**, choose **Share Snapshot**.
5. Choose one of the following options for **DB snapshot visibility**.
 - If the source is unencrypted, choose **Public** to permit all AWS accounts to restore a DB instance from your manual DB snapshot, or choose **Private** to permit only AWS accounts that you specify to restore a DB instance from your manual DB snapshot.

Warning

If you set **DB snapshot visibility** to **Public**, all AWS accounts can restore a DB instance from your manual DB snapshot and have access to your data. Do not share any manual DB snapshots that contain private information as **Public**.

- If the source is encrypted, **DB snapshot visibility** is set as **Private** because encrypted snapshots can't be shared as public.
6. For **AWS Account ID**, type the AWS account identifier for an account that you want to permit to restore a DB instance from your manual snapshot, and then choose **Add**. Repeat to include additional AWS account identifiers, up to 20 AWS accounts.

If you make an error when adding an AWS account identifier to the list of permitted accounts, you can delete it from the list by choosing **Delete** at the right of the incorrect AWS account identifier.

Snapshot permissions

Preferences

You are sharing an unencrypted DB snapshot. When you share an unencrypted DB snapshot, you give the other account permission to make a copy of the DB snapshot and to restore a database from your DB snapshot.

DB snapshot

testoracletags-snap

DB snapshot visibility

- Private
 Public

AWS account ID

Add

AWS account ID

Delete

Please add AWS account ID

Cancel

Save

- After you have added identifiers for all of the AWS accounts that you want to permit to restore the manual snapshot, choose **Save** to save your changes.

To stop sharing a manual DB snapshot with an AWS account

- Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
- In the navigation pane, choose **Snapshots**.
- Select the manual snapshot that you want to stop sharing.
- Choose **Actions**, and then choose **Share Snapshot**.
- To remove permission for an AWS account, choose **Delete** for the AWS account identifier for that account from the list of authorized accounts.

Snapshot permissions

Preferences

You are sharing an unencrypted DB snapshot. When you share an unencrypted DB snapshot, you give the other account permission to make a copy of the DB snapshot and to restore a database from your DB snapshot.

DB snapshot

testoracletags-snap

DB snapshot visibility

- Private
- Public

AWS account ID

Add

AWS account ID

Delete

Delete

Cancel

Save

6. Choose **Save** to save your changes.

AWS CLI

To share a DB snapshot, use the `aws rds modify-db-snapshot-attribute` command. Use the `--values-to-add` parameter to add a list of the IDs for the AWS accounts that are authorized to restore the manual snapshot.

Example of sharing a snapshot with a single account

The following example enables AWS account identifier 123456789012 to restore the DB snapshot named db7-snapshot.

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier db7-snapshot \
--attribute-name restore \
--values-to-add 123456789012
```

For Windows:

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier db7-snapshot ^
--attribute-name restore ^
--values-to-add 123456789012
```

Example of sharing a snapshot with multiple accounts

The following example enables two AWS account identifiers, 111122223333 and 444455556666, to restore the DB snapshot named manual-snapshot1.

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-add {"111122223333","444455556666"}
```

For Windows:

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-add "[\"111122223333\", \"444455556666\"]"
```

Note

When using the Windows command prompt, you must escape double quotes ("") in JSON code by prefixing them with a backslash (\).

To remove an AWS account identifier from the list, use the --values-to-remove parameter.

Example of stopping snapshot sharing

The following example prevents AWS account ID 444455556666 from restoring the snapshot.

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-remove 444455556666
```

For Windows:

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-remove 444455556666
```

To list the AWS accounts enabled to restore a snapshot, use the [describe-db-snapshot-attributes](#) AWS CLI command.

RDS API

You can also share a manual DB snapshot with other AWS accounts by using the Amazon RDS API. To do so, call the [ModifyDBSnapshotAttribute](#) operation. Specify `restore` for `AttributeName`, and use the `ValuesToAdd` parameter to add a list of the IDs for the AWS accounts that are authorized to restore the manual snapshot.

To make a manual snapshot public and restorable by all AWS accounts, use the value `all`. However, take care not to add the `all` value for any manual snapshots that contain private information that you don't want to be available to all AWS accounts. Also, don't specify `all` for encrypted snapshots, because making such snapshots public isn't supported.

To remove sharing permission for an AWS account, use the [ModifyDBSnapshotAttribute](#) operation with `AttributeName` set to `restore` and the `ValuesToRemove` parameter. To mark a manual snapshot as private, remove the value `all` from the values list for the `restore` attribute.

To list all of the AWS accounts permitted to restore a snapshot, use the [DescribeDBSnapshotAttributes](#) API operation.

Exporting DB snapshot data to Amazon S3

You can export DB snapshot data to an Amazon S3 bucket. The export process runs in the background and doesn't affect the performance of your active DB instance.

When you export a DB snapshot, Amazon RDS extracts data from the snapshot and stores it in an Amazon S3 bucket. The data is stored in an Apache Parquet format that is compressed and consistent.

You can export all types of DB snapshots—including manual snapshots, automated system snapshots, and snapshots created by the AWS Backup service. By default, all data in the snapshot is exported. However, you can choose to export specific sets of databases, schemas, or tables.

After the data is exported, you can analyze the exported data directly through tools like Amazon Athena or Amazon Redshift Spectrum. For more information on using Athena to read Parquet data, see [Parquet SerDe](#) in the *Amazon Athena User Guide*. For more information on using Redshift Spectrum to read Parquet data, see [COPY from columnar data formats](#) in the *Amazon Redshift Database Developer Guide*.

Topics

- [Region and version availability \(p. 481\)](#)
- [Limitations \(p. 481\)](#)
- [Overview of exporting snapshot data \(p. 482\)](#)
- [Setting up access to an Amazon S3 bucket \(p. 483\)](#)
- [Using a cross-account AWS KMS key for encrypting Amazon S3 exports \(p. 485\)](#)
- [Exporting a DB snapshot to an Amazon S3 bucket \(p. 486\)](#)
- [Monitoring snapshot exports \(p. 489\)](#)
- [Canceling a snapshot export task \(p. 490\)](#)
- [Failure messages for Amazon S3 export tasks \(p. 491\)](#)
- [Troubleshooting PostgreSQL permissions errors \(p. 492\)](#)
- [File naming convention \(p. 492\)](#)
- [Data conversion when exporting to an Amazon S3 bucket \(p. 493\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine and across AWS Regions. For more information on version and Region availability with exporting snapshots to S3, see [Export snapshots to S3 \(p. 95\)](#).

Limitations

Exporting DB snapshot data to Amazon S3 has the following limitations:

- Exporting snapshots from DB instances that use magnetic storage isn't supported.
- The following characters in the S3 file path are converted to underscores (_) during export:

\ ` " (space)

- If a database, schema, or table has characters in its name other than the following, partial export isn't supported. However, you can export the entire DB snapshot.
 - Latin letters (A–Z)
 - Digits (0–9)
 - Dollar symbol (\$)

- Underscore (_)
- Spaces () and certain characters aren't supported in database table column names. Tables with the following characters in column names are skipped during export:

```
, ; { } ( ) \n \t = (space)
```

- Tables with slashes (/) in their names are skipped during export.
- If the data contains a large object, such as a BLOB or CLOB, that is close to or greater than 500 MB, then the export fails.
- If a table contains a large row that is close to or greater than 2 GB, then the table is skipped during export.
- We strongly recommend that you use a unique name for each export task. If you don't use a unique task name, you might receive the following error message:

ExportTaskAlreadyExistsFault: An error occurred (ExportTaskAlreadyExists) when calling the StartExportTask operation: The export task with the ID **xxxxx** already exists.

- You can delete a snapshot while you're exporting its data to S3, but you're still charged for the storage costs for that snapshot until the export task has completed.
- You can't restore exported snapshot data from S3 to a new DB instance.

Overview of exporting snapshot data

You use the following process to export DB snapshot data to an Amazon S3 bucket. For more details, see the following sections.

1. Identify the snapshot to export.

Use an existing automated or manual snapshot, or create a manual snapshot of a DB instance.

2. Set up access to the Amazon S3 bucket.

A *bucket* is a container for Amazon S3 objects or files. To provide the information to access a bucket, take the following steps:

- a. Identify the S3 bucket where the snapshot is to be exported to. The S3 bucket must be in the same AWS Region as the snapshot. For more information, see [Identifying the Amazon S3 bucket for export \(p. 483\)](#).
- b. Create an AWS Identity and Access Management (IAM) role that grants the snapshot export task access to the S3 bucket. For more information, see [Providing access to an Amazon S3 bucket using an IAM role \(p. 483\)](#).
3. Create a symmetric encryption AWS KMS key for the server-side encryption. The KMS key is used by the snapshot export task to set up AWS KMS server-side encryption when writing the export data to S3. For more information, see [Encrypting Amazon RDS resources \(p. 2000\)](#).

The KMS key is also used for local disk encryption at rest on Amazon EC2. In addition, if you have a deny statement in your KMS key policy, make sure to explicitly exclude the AWS service principal `export.rds.amazonaws.com`.

You can use a KMS key within your AWS account, or you can use a cross-account KMS key. For more information, see [Using a cross-account AWS KMS key for encrypting Amazon S3 exports \(p. 485\)](#).

4. Export the snapshot to Amazon S3 using the console or the `start-export-task` CLI command. For more information, see [Exporting a DB snapshot to an Amazon S3 bucket \(p. 486\)](#).
5. To access your exported data in the Amazon S3 bucket, see [Uploading, downloading, and managing objects in the Amazon Simple Storage Service User Guide](#).

Setting up access to an Amazon S3 bucket

To export DB snapshot data to an Amazon S3 file, you first give the snapshot permission to access the Amazon S3 bucket. You then create an IAM role to allow the Amazon RDS service to write to the Amazon S3 bucket.

Topics

- [Identifying the Amazon S3 bucket for export \(p. 483\)](#)
- [Providing access to an Amazon S3 bucket using an IAM role \(p. 483\)](#)
- [Using a cross-account Amazon S3 bucket \(p. 485\)](#)

Identifying the Amazon S3 bucket for export

Identify the Amazon S3 bucket to export the DB snapshot to. Use an existing S3 bucket or create a new S3 bucket.

Note

The S3 bucket to export to must be in the same AWS Region as the snapshot.

For more information about working with Amazon S3 buckets, see the following in the *Amazon Simple Storage Service User Guide*:

- [How do I view the properties for an S3 bucket?](#)
- [How do I enable default encryption for an Amazon S3 bucket?](#)
- [How do I create an S3 bucket?](#)

Providing access to an Amazon S3 bucket using an IAM role

Before you export DB snapshot data to Amazon S3, give the snapshot export tasks write-access permission to the Amazon S3 bucket.

To grant this permission, create an IAM policy that provides access to the bucket, then create an IAM role and attach the policy to the role. You later assign the IAM role to your snapshot export task.

Important

If you plan to use the AWS Management Console to export your snapshot, you can choose to create the IAM policy and the role automatically when you export the snapshot. For instructions, see [Exporting a DB snapshot to an Amazon S3 bucket \(p. 486\)](#).

To give DB snapshot tasks access to Amazon S3

1. Create an IAM policy. This policy provides the bucket and object permissions that allow your snapshot export task to access Amazon S3.

In the policy, include the following required actions to allow the transfer of files from Amazon RDS to an S3 bucket:

- `s3:PutObject*`
- `s3:GetObject*`
- `s3>ListBucket`
- `s3>DeleteObject*`
- `s3:GetBucketLocation`

In the policy, include the following resources to identify the S3 bucket and objects in the bucket. The following list of resources shows the Amazon Resource Name (ARN) format for accessing Amazon S3.

- `arn:aws:s3:::your-s3-bucket`
- `arn:aws:s3:::your-s3-bucket/*`

For more information on creating an IAM policy for Amazon RDS, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#). See also [Tutorial: Create and attach your first customer managed policy](#) in the *IAM User Guide*.

The following AWS CLI command creates an IAM policy named `ExportPolicy` with these options. It grants access to a bucket named `your-s3-bucket`.

Note

After you create the policy, note the ARN of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

```
aws iam create-policy --policy-name ExportPolicy --policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "ExportPolicy",  
            "Effect": "Allow",  
            "Action": [  
                "s3:PutObject*",  
                "s3>ListBucket",  
                "s3:GetObject*",  
                "s3>DeleteObject*",  
                "s3:GetBucketLocation"  
            ],  
            "Resource": [  
                "arn:aws:s3:::your-s3-bucket",  
                "arn:aws:s3:::your-s3-bucket/*"  
            ]  
        }  
    ]  
}'
```

2. Create an IAM role, so that Amazon RDS can assume this IAM role on your behalf to access your Amazon S3 buckets. For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

The following example shows using the AWS CLI command to create a role named `rds-s3-export-role`.

```
aws iam create-role --role-name rds-s3-export-role --assume-role-policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "export.rds.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}'
```

3. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created earlier to the role named `rds-s3-export-role`. Replace `your-policy-arn` with the policy ARN that you noted in an earlier step.

```
aws iam attach-role-policy --policy-arn your-policy-arn --role-name rds-s3-export-role
```

Using a cross-account Amazon S3 bucket

You can use Amazon S3 buckets across AWS accounts. To use a cross-account bucket, add a bucket policy to allow access to the IAM role that you're using for the S3 exports. For more information, see [Example 2: Bucket owner granting cross-account bucket permissions](#).

- Attach a bucket policy to your bucket, as shown in the following example.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::123456789012:role/Admin"  
            },  
            "Action": [  
                "s3:PutObject*",  
                "s3>ListBucket",  
                "s3:GetObject*",  
                "s3>DeleteObject*",  
                "s3:GetBucketLocation"  
            ],  
            "Resource": [  
                "arn:aws:s3:::mycrossaccountbucket",  
                "arn:aws:s3:::mycrossaccountbucket/*"  
            ]  
        }  
    ]  
}
```

Using a cross-account AWS KMS key for encrypting Amazon S3 exports

You can use a cross-account AWS KMS key to encrypt Amazon S3 exports. First, you add a key policy to the local account, then you add IAM policies in the external account. For more information, see [Allowing users in other accounts to use a KMS key](#).

To use a cross-account KMS key

1. Add a key policy to the local account.

The following example gives `ExampleRole` and `ExampleUser` in the external account `444455556666` permissions in the local account `123456789012`.

```
{  
    "Sid": "Allow an external account to use this KMS key",  
    "Effect": "Allow",  
    "Principal": {
```

```
        "AWS": [
            "arn:aws:iam::444455556666:role/ExampleRole",
            "arn:aws:iam::444455556666:user/ExampleUser"
        ],
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms>CreateGrant",
            "kms:DescribeKey",
            "kms:RetireGrant"
        ],
        "Resource": "*"
    }
```

2. Add IAM policies to the external account.

The following example IAM policy allows the principal to use the KMS key in account 123456789012 for cryptographic operations. To give this permission to ExampleRole and ExampleUser in account 444455556666, [attach the policy](#) to them in that account.

```
{
    "Sid": "Allow use of KMS key in account 123456789012",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms>CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant"
    ],
    "Resource": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Exporting a DB snapshot to an Amazon S3 bucket

You can have up to five concurrent DB snapshot export tasks in progress per AWS account.

Note

Exporting RDS snapshots can take a while depending on your database type and size. The export task first restores and scales the entire database before extracting the data to Amazon S3. The task's progress during this phase displays as **Starting**. When the task switches to exporting data to S3, progress displays as **In progress**.

The time it takes for the export to complete depends on the data stored in the database. For example, tables with well-distributed numeric primary key or index columns export the fastest. Tables that don't contain a column suitable for partitioning and tables with only one index on a string-based column take longer. This longer export time occurs because the export uses a slower single-threaded process.

You can export a DB snapshot to Amazon S3 using the AWS Management Console, the AWS CLI, or the RDS API.

If you use a Lambda function to export a snapshot, add the kms:DescribeKey action to the Lambda function policy. For more information, see [AWS Lambda permissions](#).

Console

The **Export to Amazon S3** console option appears only for snapshots that can be exported to Amazon S3. A snapshot might not be available for export because of the following reasons:

- The DB engine isn't supported for S3 export.
- The DB instance version isn't supported for S3 export.
- S3 export isn't supported in the AWS Region where the snapshot was created.

To export a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. From the tabs, choose the type of snapshot that you want to export.
4. In the list of snapshots, choose the snapshot that you want to export.
5. For **Actions**, choose **Export to Amazon S3**.

The **Export to Amazon S3** window appears.

6. For **Export identifier**, enter a name to identify the export task. This value is also used for the name of the file created in the S3 bucket.
7. Choose the data to be exported:
 - Choose **All** to export all data in the snapshot.
 - Choose **Partial** to export specific parts of the snapshot. To identify which parts of the snapshot to export, enter one or more databases, schemas, or tables for **Identifiers**, separated by spaces.

Use the following format:

```
database[.schema][.table] database2[.schema2][.table2] ... databasen[.scheman]  
[.tablen]
```

For example:

```
mydatabase mydatabase2.myschema1 mydatabase2.myschema2.mytable1  
mydatabase2.myschema2.mytable2
```

8. For **S3 bucket**, choose the bucket to export to.

To assign the exported data to a folder path in the S3 bucket, enter the optional path for **S3 prefix**.

9. For **IAM role**, either choose a role that grants you write access to your chosen S3 bucket, or create a new role.
 - If you created a role by following the steps in [Providing access to an Amazon S3 bucket using an IAM role \(p. 483\)](#), choose that role.
 - If you didn't create a role that grants you write access to your chosen S3 bucket, then choose **Create a new role** to create the role automatically. Next, enter a name for the role in **IAM role name**.
10. For **AWS KMS key**, enter the ARN for the key to use for encrypting the exported data.
11. Choose **Export to Amazon S3**.

AWS CLI

To export a DB snapshot to Amazon S3 using the AWS CLI, use the [start-export-task](#) command with the following required options:

- --export-task-identifier
- --source-arn
- --s3-bucket-name
- --iam-role-arn
- --kms-key-id

In the following examples, the snapshot export task is named *my-snapshot-export*, which exports a snapshot to an S3 bucket named *my-export-bucket*.

Example

For Linux, macOS, or Unix:

```
aws rds start-export-task \
  --export-task-identifier my-snapshot-export \
  --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name \
  --s3-bucket-name my-export-bucket \
  --iam-role-arn iam-role \
  --kms-key-id my-key
```

For Windows:

```
aws rds start-export-task ^
  --export-task-identifier my-snapshot-export ^
  --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name ^
  --s3-bucket-name my-export-bucket ^
  --iam-role-arn iam-role ^
  --kms-key-id my-key
```

Sample output follows.

```
{  
    "Status": "STARTING",  
    "IamRoleArn": "iam-role",  
    "ExportTime": "2019-08-12T01:23:53.109Z",  
    "S3Bucket": "my-export-bucket",  
    "PercentProgress": 0,  
    "KmsKeyId": "my-key",  
    "ExportTaskIdentifier": "my-snapshot-export",  
    "TotalExtractedDataInGB": 0,  
    "TaskStartTime": "2019-11-13T19:46:00.173Z",  
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name"  
}
```

To provide a folder path in the S3 bucket for the snapshot export, include the `--s3-prefix` option in the [start-export-task](#) command.

RDS API

To export a DB snapshot to Amazon S3 using the Amazon RDS API, use the [StartExportTask](#) operation with the following required parameters:

- ExportTaskIdentifier

- `SourceArn`
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

Monitoring snapshot exports

You can monitor DB snapshot exports using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To monitor DB snapshot exports

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. To view the list of snapshot exports, choose the **Exports in Amazon S3** tab.
4. To view information about a specific snapshot export, choose the export task.

AWS CLI

To monitor DB snapshot exports using the AWS CLI, use the `describe-export-tasks` command.

The following example shows how to display current information about all of your snapshot exports.

Example

```
aws rds describe-export-tasks

{
    "ExportTasks": [
        {
            "Status": "CANCELED",
            "TaskEndTime": "2019-11-01T17:36:46.961Z",
            "S3Prefix": "something",
            "ExportTime": "2019-10-24T20:23:48.364Z",
            "S3Bucket": "examplebucket",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:AWS Region:123456789012:key/K7MDENG/bPxRfiCYEXAMPLEKEY",
            "ExportTaskIdentifier": "anewtest",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "TaskStartTime": "2019-10-25T19:10:58.885Z",
            "SourceArn": "arn:aws:rds:AWS Region:123456789012:snapshot:parameter-groups-test"
        },
        {
            "Status": "COMPLETE",
            "TaskEndTime": "2019-10-31T21:37:28.312Z",
            "WarningMessage": "{\"skippedTables\":[],\"skippedObjectives\":[],\"general\": [{\"reason\":\"FAILED_TO_EXTRACT_TABLES_LIST_FOR_DATABASE\"}]}",
            "S3Prefix": "",
            "ExportTime": "2019-10-31T06:44:53.452Z",
            "S3Bucket": "examplebucket1",
            "PercentProgress": 100,
            "KmsKeyId": "arn:aws:kms:AWS Region:123456789012:key/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
        }
    ]
}
```

```
"ExportTaskIdentifier": "thursday-events-test",
"IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
"TotalExtractedDataInGB": 263,
"TaskStartTime": "2019-10-31T20:58:06.998Z",
"SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-31-06-44"
},
{
    "Status": "FAILED",
    "TaskEndTime": "2019-10-31T02:12:36.409Z",
    "FailureCause": "The S3 bucket edgcuc-export isn't located in the current AWS Region. Please, review your S3 bucket name and retry the export.",
    "S3Prefix": "",
    "ExportTime": "2019-10-30T06:45:04.526Z",
    "S3Bucket": "examplebucket2",
    "PercentProgress": 0,
    "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
    "ExportTaskIdentifier": "wednesday-afternoon-test",
    "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-10-30T22:43:40.034Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-30-06-45"
}
]
```

To display information about a specific snapshot export, include the `--export-task-identifier` option with the `describe-export-tasks` command. To filter the output, include the `--Filters` option. For more options, see the [describe-export-tasks](#) command.

RDS API

To display information about DB snapshot exports using the Amazon RDS API, use the [DescribeExportTasks](#) operation.

To track completion of the export workflow or to initiate another workflow, you can subscribe to Amazon Simple Notification Service topics. For more information on Amazon SNS, see [Working with Amazon RDS event notification \(p. 650\)](#).

Canceling a snapshot export task

You can cancel a DB snapshot export task using the AWS Management Console, the AWS CLI, or the RDS API.

Note

Canceling a snapshot export task doesn't remove any data that was exported to Amazon S3. For information about how to delete the data using the console, see [How do I delete objects from an S3 bucket?](#) To delete the data using the CLI, use the `delete-object` command.

Console

To cancel a snapshot export task

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the **Exports in Amazon S3** tab.
4. Choose the snapshot export task that you want to cancel.
5. Choose **Cancel**.

6. Choose **Cancel export task** on the confirmation page.

AWS CLI

To cancel a snapshot export task using the AWS CLI, use the [cancel-export-task](#) command. The command requires the `--export-task-identifier` option.

Example

```
aws rds cancel-export-task --export-task-identifier my_export
{
    "Status": "CANCELING",
    "S3Prefix": "",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "examplebucket",
    "PercentProgress": 0,
    "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "ExportTaskIdentifier": "my_export",
    "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:export-example-1"
}
```

RDS API

To cancel a snapshot export task using the Amazon RDS API, use the [CancelExportTask](#) operation with the `ExportTaskIdentifier` parameter.

Failure messages for Amazon S3 export tasks

The following table describes the messages that are returned when Amazon S3 export tasks fail.

Failure message	Description
An unknown internal error occurred.	The task has failed because of an unknown error, exception, or failure.
An unknown internal error occurred writing the export task's metadata to the S3 bucket [bucket name].	The task has failed because of an unknown error, exception, or failure.
The RDS export failed to write the export task's metadata because it can't assume the IAM role [role ARN].	The export task assumes your IAM role to validate whether it is allowed to write metadata to your S3 bucket. If the task can't assume your IAM role, it fails.
The RDS export failed to write the export task's metadata to the S3 bucket [bucket name] using the IAM role [role ARN] with the KMS key [key ID]. Error code: [error code]	One or more permissions are missing, so the export task can't access the S3 bucket. This failure message is raised when receiving one of the following error codes: <ul style="list-style-type: none">• <code>AWSecurityTokenServiceException</code> with the error code <code>AccessDenied</code>• <code>AmazonS3Exception</code> with the error code <code>NoSuchBucket</code>, <code>AccessDenied</code>, <code>KMS.InvalidStateException</code>, <code>403 Forbidden</code>, or <code>KMS.DisabledException</code>

Failure message	Description
	These error codes indicate settings are misconfigured for the IAM role, S3 bucket, or KMS key.
The IAM role [role ARN] isn't authorized to call [S3 action] on the S3 bucket [bucket name]. Review your permissions and retry the export.	The IAM policy is misconfigured. Permission for the specific S3 action on the S3 bucket is missing, which causes the export task to fail.
KMS key check failed. Check the credentials on your KMS key and try again.	The KMS key credential check failed.
S3 credential check failed. Check the permissions on your S3 bucket and IAM policy.	The S3 credential check failed.
The S3 bucket [bucket name] isn't valid. Either it isn't located in the current AWS Region or it doesn't exist. Review your S3 bucket name and retry the export.	The S3 bucket is invalid.
The S3 bucket [bucket name] isn't located in the current AWS Region. Review your S3 bucket name and retry the export.	The S3 bucket is in the wrong AWS Region.

Troubleshooting PostgreSQL permissions errors

When exporting PostgreSQL databases to Amazon S3, you might see a PERMISSIONS_D0_NOT_EXIST error stating that certain tables were skipped. This error usually occurs when the superuser, which you specified when creating the DB instance, doesn't have permissions to access those tables.

To fix this error, run the following command:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA schema_name TO superuser_name
```

For more information on superuser privileges, see [Master user account privileges \(p. 2087\)](#).

File naming convention

Exported data for specific tables is stored in the format *base_prefix/files*, where the base prefix is the following:

export_identifier/database_name/schema_name.table_name/

For example:

`export-1234567890123-459/rdststdb/rdststdb.DataInsert_7ADB5D19965123A2/`

There are two conventions for how files are named. The current convention is the following:

partition_index/part-00000-random_uuid.format-based_extension

For example:

```
1/part-00000-c5a881bb-58ff-4ee6-1111-b41ecff340a3-c000.gz.parquet
2/part-00000-d7a881cc-88cc-5ab7-2222-c41ecab340a4-c000.gz.parquet
3/part-00000-f5a991ab-59aa-7fa6-3333-d41eccd340a7-c000.gz.parquet
```

The older convention is the following:

```
part-partition_index-random_uuid.format-based_extension
```

For example:

```
part-00000-c5a881bb-58ff-4ee6-1111-b41ecff340a3-c000.gz.parquet
part-00001-d7a881cc-88cc-5ab7-2222-c41ecab340a4-c000.gz.parquet
part-00002-f5a991ab-59aa-7fa6-3333-d41eccd340a7-c000.gz.parquet
```

The file naming convention is subject to change. Therefore, when reading target tables, we recommend that you read everything inside the base prefix for the table.

Data conversion when exporting to an Amazon S3 bucket

When you export a DB snapshot to an Amazon S3 bucket, Amazon RDS converts data to, exports data in, and stores data in the Parquet format. For more information about Parquet, see the [Apache Parquet](#) website.

Parquet stores all data as one of the following primitive types:

- BOOLEAN
- INT32
- INT64
- INT96
- FLOAT
- DOUBLE
- BYTE_ARRAY – A variable-length byte array, also known as binary
- FIXED_LEN_BYTE_ARRAY – A fixed-length byte array used when the values have a constant size

The Parquet data types are few to reduce the complexity of reading and writing the format. Parquet provides logical types for extending primitive types. A *logical type* is implemented as an annotation with the data in a LogicalType metadata field. The logical type annotation explains how to interpret the primitive type.

When the STRING logical type annotates a BYTE_ARRAY type, it indicates that the byte array should be interpreted as a UTF-8 encoded character string. After an export task completes, Amazon RDS notifies you if any string conversion occurred. The underlying data exported is always the same as the data from the source. However, due to the encoding difference in UTF-8, some characters might appear different from the source when read in tools such as Athena.

For more information, see [Parquet logical type definitions](#) in the Parquet documentation.

Topics

- [MySQL and MariaDB data type mapping to Parquet \(p. 494\)](#)
- [PostgreSQL data type mapping to Parquet \(p. 496\)](#)

MySQL and MariaDB data type mapping to Parquet

The following table shows the mapping from MySQL and MariaDB data types to Parquet data types when data is converted and exported to Amazon S3.

Source data type	Parquet primitive type	Logical type annotation	Conversion notes
Numeric data types			
BIGINT	INT64		
BIGINT UNSIGNED	FIXED_LEN_BYTE_ARRAY(9)DECIMAL(20,0)		Parquet supports only signed types, so the mapping requires an additional byte (8 plus 1) to store the BIGINT_UNSIGNED type.
BIT	BYTE_ARRAY		
DECIMAL	INT32	DECIMAL(p,s)	If the source value is less than 2^{31} , it's stored as INT32.
	INT64	DECIMAL(p,s)	If the source value is 2^{31} or greater, but less than 2^{63} , it's stored as INT64.
	FIXED_LEN_BYTE_ARRAY(N)DECIMAL(p,s)		If the source value is 2^{63} or greater, it's stored as FIXED_LEN_BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet doesn't support Decimal precision greater than 38. The Decimal value is converted to a string in a BYTE_ARRAY type and encoded as UTF8.
DOUBLE	DOUBLE		
FLOAT	DOUBLE		
INT	INT32		
INT UNSIGNED	INT64		
MEDIUMINT	INT32		
MEDIUMINT UNSIGNED	INT64		
NUMERIC	INT32	DECIMAL(p,s)	If the source value is less than 2^{31} , it's stored as INT32.

Source data type	Parquet primitive type	Logical type annotation	Conversion notes
	INT64	DECIMAL(p,s)	If the source value is 2^{31} or greater, but less than 2^{63} , it's stored as INT64.
	FIXED_LEN_ARRAY(N)	DECIMAL(p,s)	If the source value is 2^{63} or greater, it's stored as FIXED_LEN_BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet doesn't support Numeric precision greater than 38. This Numeric value is converted to a string in a BYTE_ARRAY type and encoded as UTF8.
SMALLINT	INT32		
SMALLINT UNSIGNED	INT32		
TINYINT	INT32		
TINYINT UNSIGNED	INT32		
String data types			
BINARY	BYTE_ARRAY		
BLOB	BYTE_ARRAY		
CHAR	BYTE_ARRAY		
ENUM	BYTE_ARRAY	STRING	
LINESTRING	BYTE_ARRAY		
LONGBLOB	BYTE_ARRAY		
LONGTEXT	BYTE_ARRAY	STRING	
MEDIUMBLOB	BYTE_ARRAY		
MEDIUMTEXT	BYTE_ARRAY	STRING	
MULTILINESTRING	BYTE_ARRAY		
SET	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TINYBLOB	BYTE_ARRAY		
TINYTEXT	BYTE_ARRAY	STRING	
VARBINARY	BYTE_ARRAY		
VARCHAR	BYTE_ARRAY	STRING	
Date and time data types			

Source data type	Parquet primitive type	Logical type annotation	Conversion notes
DATE	BYTE_ARRAY	STRING	A date is converted to a string in a BYTE_ARRAY type and encoded as UTF8.
DATETIME	INT64	TIMESTAMP_MICROS	
TIME	BYTE_ARRAY	STRING	A TIME type is converted to a string in a BYTE_ARRAY and encoded as UTF8.
TIMESTAMP	INT64	TIMESTAMP_MICROS	
YEAR	INT32		
Geometric data types			
GEOMETRY	BYTE_ARRAY		
GEOMETRYCOLLECTION	BYTE_ARRAY		
MULTIPOINT	BYTE_ARRAY		
MULTIPOLYGON	BYTE_ARRAY		
POINT	BYTE_ARRAY		
POLYGON	BYTE_ARRAY		
JSON data type			
JSON	BYTE_ARRAY	STRING	

PostgreSQL data type mapping to Parquet

The following table shows the mapping from PostgreSQL data types to Parquet data types when data is converted and exported to Amazon S3.

PostgreSQL data type	Parquet primitive type	Logical type annotation	Mapping notes
Numeric data types			
BIGINT	INT64		
BIGSERIAL	INT64		
DECIMAL	BYTE_ARRAY	STRING	A DECIMAL type is converted to a string in a BYTE_ARRAY type and encoded as UTF8. This conversion is to avoid complications due to data precision and

PostgreSQL data type	Parquet primitive type	Logical type annotation	Mapping notes
			data values that are not a number (NaN).
DOUBLE PRECISION	DOUBLE		
INTEGER	INT32		
MONEY	BYTE_ARRAY	STRING	
REAL	FLOAT		
SERIAL	INT32		
SMALLINT	INT32	INT_16	
SMALLSERIAL	INT32	INT_16	
String and related data types			
ARRAY	BYTE_ARRAY	STRING	An array is converted to a string and encoded as BINARY (UTF8). This conversion is to avoid complications due to data precision, data values that are not a number (NaN), and time data values.
BIT	BYTE_ARRAY	STRING	
BIT VARYING	BYTE_ARRAY	STRING	
BYTEA	BINARY		
CHAR	BYTE_ARRAY	STRING	
CHAR(N)	BYTE_ARRAY	STRING	
ENUM	BYTE_ARRAY	STRING	
NAME	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TEXT SEARCH	BYTE_ARRAY	STRING	
VARCHAR(N)	BYTE_ARRAY	STRING	
XML	BYTE_ARRAY	STRING	
Date and time data types			
DATE	BYTE_ARRAY	STRING	
INTERVAL	BYTE_ARRAY	STRING	
TIME	BYTE_ARRAY	STRING	

PostgreSQL data type	Parquet primitive type	Logical type annotation	Mapping notes
TIME WITH TIME ZONE	BYTE_ARRAY	STRING	
TIMESTAMP	BYTE_ARRAY	STRING	
TIMESTAMP WITH TIME ZONE	BYTE_ARRAY	STRING	
Geometric data types			
BOX	BYTE_ARRAY	STRING	
CIRCLE	BYTE_ARRAY	STRING	
LINE	BYTE_ARRAY	STRING	
LINESEGMENT	BYTE_ARRAY	STRING	
PATH	BYTE_ARRAY	STRING	
POINT	BYTE_ARRAY	STRING	
POLYGON	BYTE_ARRAY	STRING	
JSON data types			
JSON	BYTE_ARRAY	STRING	
JSONB	BYTE_ARRAY	STRING	
Other data types			
BOOLEAN	BOOLEAN		
CIDR	BYTE_ARRAY	STRING	Network data type
COMPOSITE	BYTE_ARRAY	STRING	
DOMAIN	BYTE_ARRAY	STRING	
INET	BYTE_ARRAY	STRING	Network data type
MACADDR	BYTE_ARRAY	STRING	
OBJECT IDENTIFIER	N/A		
PG_LSN	BYTE_ARRAY	STRING	
RANGE	BYTE_ARRAY	STRING	
UUID	BYTE_ARRAY	STRING	

Restoring a DB instance to a specified time

You can restore a DB instance to a specific point in time, creating a new DB instance.

When you restore a DB instance to a point in time, you can choose the default virtual private cloud (VPC) security group. Or you can apply a custom VPC security group to your DB instance.

Restored DB instances are automatically associated with the default DB parameter and option groups. However, you can apply a custom parameter group and option group by specifying them during a restore.

RDS uploads transaction logs for DB instances to Amazon S3 every five minutes. To see the latest restorable time for a DB instance, use the AWS CLI `describe-db-instances` command and look at the value returned in the `LatestRestorableTime` field for the DB instance. To see the latest restorable time for each DB instance in the Amazon RDS console, choose **Automated backups**.

You can restore to any point in time within your backup retention period. To see the earliest restorable time for each DB instance, choose **Automated backups** in the Amazon RDS console.

DB Name	Earliest restorable time	Latest restorable time	Engine	Encrypted
database-1	December 27th 2020, 9:42:48 am UTC	January 4th 2021, 6:25:01 pm UTC	sqlserver-se	No
database-1-sast	December 31st 2020, 9:18:52 am UTC	January 8th 2021, 2:44:01 pm UTC	sqlserver-ex	No
database-2	December 24th 2020, 11:58:45 am UTC	January 8th 2021, 2:46:01 pm UTC	sqlserver-se	Yes
database-3	December 31st 2020, 9:51:23 am UTC	January 8th 2021, 2:43:01 pm UTC	sqlserver-ex	No
database-6	December 31st 2020, 6:54:19 am UTC	January 8th 2021, 2:42:01 pm UTC	sqlserver-ex	No
database-7	January 1st 2021, 12:21:52 pm UTC	January 8th 2021, 2:50:00 pm UTC	mysql	No
db4-5640	January 4th 2021, 7:11:04 pm UTC	January 8th 2021, 2:50:00 pm UTC	mysql	No
myoracleinstance-from-replicated-backup	December 24th 2020, 7:49:18 am UTC	January 8th 2021, 2:47:57 pm UTC	oracle-se2	No
test2-mysql-mag-maz	January 6th 2021, 6:42:52 am UTC	January 8th 2021, 2:50:00 pm UTC	mysql	No

Note

We recommend that you restore to the same or similar DB instance size—and IOPS if using Provisioned IOPS storage—as the source DB instance. You might get an error if, for example, you choose a DB instance size with an incompatible IOPS value.

Some of the database engines used by Amazon RDS have special considerations when restoring from a point in time:

- When you restore an Oracle DB instance to a point in time, you can specify a different Oracle DB engine, license model, and DBName (SID) to be used by the new DB instance.
- When you restore a Microsoft SQL Server DB instance to a point in time, each database within that instance is restored to a point in time within 1 second of each other database within the instance. Transactions that span multiple databases within the instance might be restored inconsistently.
- For a SQL Server DB instance, the OFFLINE, EMERGENCY, and SINGLE_USER modes aren't supported. Setting any database into one of these modes causes the latest restorable time to stop moving ahead for the whole instance.
- Some actions, such as changing the recovery model of a SQL Server database, can break the sequence of logs that are used for point-in-time recovery. In some cases, Amazon RDS can detect this issue and the latest restorable time is prevented from moving forward. In other cases, such as when a SQL Server database uses the BULK_LOGGED recovery model, the break in log sequence isn't detected. It might not be possible to restore a SQL Server DB instance to a point in time if there is a break in the

log sequence. For these reasons, Amazon RDS doesn't support changing the recovery model of SQL Server databases.

You can also use AWS Backup to manage backups of Amazon RDS DB instances. If your DB instance is associated with a backup plan in AWS Backup, that backup plan is used for point-in-time recovery. Backups that were created with AWS Backup have names ending in awsbackup:*AWS-Backup-job-number*. For information about AWS Backup, see the [AWS Backup Developer Guide](#).

Note

Information in this topic applies to Amazon RDS. For information on restoring an Amazon Aurora DB cluster, see [Restoring a DB cluster to a specified time](#).

You can restore a DB instance to a point in time using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore a DB instance to a specified time

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Automated backups**.
The automated backups are displayed on the **Current Region** tab.
3. Choose the DB instance that you want to restore.
4. For **Actions**, choose **Restore to point in time**.
The **Restore to point in time** window appears.
5. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time to which you want to restore the instance.

Note

Times are shown in your local time zone, which is indicated by an offset from Coordinated Universal Time (UTC). For example, UTC-5 is Eastern Standard Time/Central Daylight Time.

6. For **DB instance identifier**, enter the name of the target restored DB instance. The name must be unique.
7. Choose other options as needed, such as DB instance class, storage, and whether you want to use storage autoscaling.

For information about each setting, see [Settings for DB instances \(p. 237\)](#).

8. Choose **Restore to point in time**.

AWS CLI

To restore a DB instance to a specified time, use the AWS CLI command `restore-db-instance-to-point-in-time` to create a new DB instance. This example also enables storage autoscaling.

You can specify other settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-to-point-in-time \
```

```
--source-db-instance-identifier mysourcedbinstance \
--target-db-instance-identifier mytargetdbinstance \
--restore-time 2017-10-14T23:45:00.000Z \
--max-allocated-storage 1000
```

For Windows:

```
aws rds restore-db-instance-to-point-in-time ^
--source-db-instance-identifier mysourcedbinstance ^
--target-db-instance-identifier mytargetdbinstance ^
--restore-time 2017-10-14T23:45:00.000Z ^
--max-allocated-storage 1000
```

RDS API

To restore a DB instance to a specified time, call the Amazon RDS API

[RestoreDBInstanceToPointInTime](#) operation with the following parameters:

- `SourceDBInstanceIdentifier`
- `TargetDBInstanceIdentifier`
- `RestoreTime`

Restoring a Multi-AZ DB cluster to a specified time

You can restore a Multi-AZ DB cluster to a specific point in time, creating a new Multi-AZ DB cluster.

RDS uploads transaction logs for Multi-AZ DB clusters to Amazon S3 continuously. You can restore to any point in time within your backup retention period. To see the earliest restorable time for a Multi-AZ DB cluster, use the AWS CLI `describe-db-clusters` command. Look at the value returned in the `EarliestRestorableTime` field for the DB cluster. To see the latest restorable time for a Multi-AZ DB cluster, look at the value returned in the `LatestRestorableTime` field for the DB cluster.

When you restore a Multi-AZ DB cluster to a point in time, you can choose the default VPC security group for your Multi-AZ DB cluster. Or you can apply a custom VPC security group to your Multi-AZ DB cluster.

Restored Multi-AZ DB clusters are automatically associated with the default DB cluster parameter group. However, you can apply a customer DB cluster parameter group by specifying it during a restore.

Note

We recommend that you restore to the same or similar Multi-AZ DB cluster size as the source DB cluster. We also recommend that you restore with the same or similar IOPS value if you're using Provisioned IOPS storage. You might get an error if, for example, you choose a DB cluster size with an incompatible IOPS value.

You can restore a Multi-AZ DB cluster to a point in time using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore a Multi-AZ DB cluster to a specified time

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the Multi-AZ DB cluster that you want to restore.
4. For **Actions**, choose **Restore to point in time**.

The **Restore to point in time** window appears.

5. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time to which you want to restore the Multi-AZ DB cluster.

Note

Times are shown in your local time zone, which is indicated by an offset from Coordinated Universal Time (UTC). For example, UTC-5 is Eastern Standard Time/Central Daylight Time.

6. For **DB cluster identifier**, enter the name for your restored Multi-AZ DB cluster.
7. In **Availability and durability**, choose **Multi-AZ DB cluster**.

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB cluster

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance

Creates a single DB instance with no standby DB instances.

8. In **DB instance class**, choose a DB instance class.

Currently, Multi-AZ DB clusters only support db.m6gd and db.r6gd DB instance classes. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).

9. For the remaining sections, specify your DB cluster settings. For information about each setting, see [Settings for creating Multi-AZ DB clusters \(p. 258\)](#).

10. Choose **Restore to point in time**.

AWS CLI

To restore a Multi-AZ DB cluster to a specified time, use the AWS CLI command [restore-db-cluster-to-point-in-time](#) to create a new Multi-AZ DB cluster.

Currently, Multi-AZ DB clusters only support db.m6gd and db.r6gd DB instance classes. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-cluster-to-point-in-time \
--source-db-cluster-identifier mysourcemultiazdbcluster \
--db-cluster-identifier mytargetmultiazdbcluster \
--restore-to-time 2021-08-14T23:45:00.000Z \
--db-cluster-instance-class db.r6gd.xlarge
```

For Windows:

```
aws rds restore-db-cluster-to-point-in-time ^
--source-db-cluster-identifier mysourcemultiazdbcluster ^
--db-cluster-identifier mytargetmultiazdbcluster ^
--restore-to-time 2021-08-14T23:45:00.000Z ^
--db-cluster-instance-class db.r6gd.xlarge
```

RDS API

To restore a DB cluster to a specified time, call the Amazon RDS API [RestoreDBClusterToPointInTime](#) operation with the following parameters:

- **SourceDBClusterIdentifier**
- **DBClusterIdentifier**

- `RestoreToTime`

Deleting a DB snapshot

You can delete DB snapshots managed by Amazon RDS when you no longer need them.

Note

To delete backups managed by AWS Backup, use the AWS Backup console. For information about AWS Backup, see the [AWS Backup Developer Guide](#).

Deleting a DB snapshot

You can delete a manual, shared, or public DB snapshot using the AWS Management Console, the AWS CLI, or the RDS API.

To delete a shared or public snapshot, you must sign in to the AWS account that owns the snapshot.

If you have automated DB snapshots that you want to delete without deleting the DB instance, change the backup retention period for the DB instance to 0. The automated snapshots are deleted when the change is applied. You can apply the change immediately if you don't want to wait until the next maintenance period. After the change is complete, you can then re-enable automatic backups by setting the backup retention period to a number greater than 0. For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If you deleted a DB instance, you can delete its automated DB snapshots by removing the automated backups for the DB instance. For information about automated backups, see [Working with backups \(p. 427\)](#).

Console

To delete a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.

The **Manual snapshots** list appears.

3. Choose the DB snapshot that you want to delete.
4. For **Actions**, choose **Delete snapshot**.
5. Choose **Delete** on the confirmation page.

AWS CLI

You can delete a DB snapshot by using the AWS CLI command `delete-db-snapshot`.

The following options are used to delete a DB snapshot.

- `--db-snapshot-identifier` – The identifier for the DB snapshot.

Example

The following code deletes the `mydbsnapshot` DB snapshot.

For Linux, macOS, or Unix:

```
aws rds delete-db-snapshot \
--db-snapshot-identifier mydbsnapshot
```

For Windows:

```
aws rds delete-db-snapshot ^
--db-snapshot-identifier mydbsnapshot
```

RDS API

You can delete a DB snapshot by using the Amazon RDS API operation [DeleteDBSnapshot](#).

The following parameters are used to delete a DB snapshot.

- **DBSnapshotIdentifier** – The identifier for the DB snapshot.

Tutorial: Restore an Amazon RDS DB instance from a DB snapshot

Often, when working with Amazon RDS you might have a DB instance that you work with occasionally but don't need full time. For example, suppose that you have a quarterly customer survey that uses an Amazon EC2 instance to host a customer survey website. You also have a DB instance that is used to store the survey results. One way to save money on such a scenario is to take a DB snapshot of the DB instance after the survey is completed. You then delete the DB instance and restore it when you need to conduct the survey again.

When you restore the DB instance, you provide the name of the DB snapshot to restore from. You then provide a name for the new DB instance that's created from the restore operation.

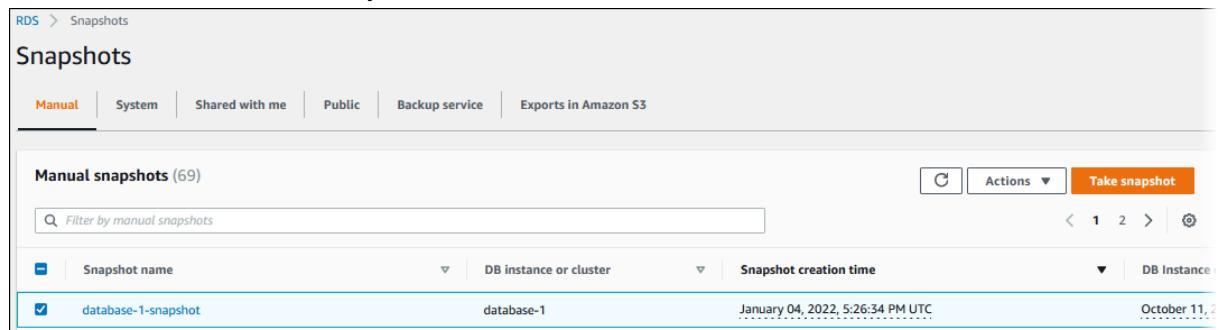
For more detailed information on restoring DB instances from snapshots, see [Restoring from a DB snapshot \(p. 452\)](#).

Restoring a DB instance from a DB snapshot

Use the following procedure to restore from a snapshot in the AWS Management Console.

To restore a DB instance from a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to restore from.
4. For **Actions**, choose **Restore snapshot**.



The **Restore snapshot** page appears.

RDS > Snapshots > Restore snapshot

Restore snapshot

You are creating a new DB instance or DB cluster from a snapshot. The default VPC security group and parameter group are selected for the new DB instance or DB cluster, but you can change these settings.

DB instance settings

DB engine: SQL Server Express Edition

License model: license-included

Settings

DB snapshot ID: database-1-snapshot

DB instance identifier: mynewdbinstance

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

5. Under **DB instance settings**, use the default settings for **DB engine** and **License model** (for Oracle or Microsoft SQL Server).
6. Under **Settings**, for **DB instance identifier** enter the unique name that you want to use for the restored DB instance, for example **mynewdbinstance**.

If you're restoring from a DB instance that you deleted after you made the DB snapshot, you can use the name of that DB instance.
7. Under **Availability & durability**, for **Multi-AZ deployment** choose whether to create a standby instance in another Availability Zone.

For this tutorial, use **No**, the default setting.
8. Under **Connectivity**, use the default settings for the following:
 - **Virtual private cloud (VPC)**
 - **DB subnet group**
 - **Public access**
 - **VPC security group (firewall)**
9. Choose the **DB instance class**.

For this tutorial, choose **Burstable classes (includes t classes)**, and then choose **db.t3.small**.
10. For **Encryption**, use the default settings.

If the source DB instance for the snapshot was encrypted, the restored DB instance is also encrypted. You can't make it unencrypted.
11. Expand **Additional configuration** at the bottom of the page.

Additional configuration

Database options

DB parameter group [Info](#)
default.sqlserver-ex-15.0

Option group [Info](#)
default:sqlserver-ex-15-00

Collation [Info](#)

Backup

Copy tags to snapshots

Log exports

Select the log types to publish to Amazon CloudWatch Logs

Error log

IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released.
The automatic upgrades occur during the maintenance window for the database.

Deletion protection

Enable deletion protection
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

12. Do the following under Database options:

- Choose the **DB parameter group**.

For this tutorial, use the default parameter group.

- Choose the **Option group**.

For this tutorial, use the default option group.

Important

In some cases, you might restore from a DB snapshot of a DB instance that uses a persistent or permanent option. If so, make sure to choose an option group that uses the same option.

- For **Deletion protection**, choose the **Enable deletion protection** check box.

13. Choose Restore DB instance.

The **Databases** page displays the restored DB instance, with a status of **Creating**.

	mynewdbinstance	Instance	SQL Server Express Edition	15.00.4073.23.v1	-	db.t3.small	
--	-----------------	----------	----------------------------	------------------	---	-------------	--

Monitoring metrics in an Amazon RDS instance

In the following sections, you can find an overview of Amazon RDS monitoring and an explanation about how to access metrics. To learn how to monitor events, logs, and database activity streams, see [Monitoring events, logs, and streams in an Amazon RDS DB instance \(p. 642\)](#).

Topics

- [Overview of monitoring metrics in Amazon RDS \(p. 511\)](#)
- [Viewing instance status and recommendations \(p. 515\)](#)
- [Viewing metrics in the Amazon RDS console \(p. 525\)](#)
- [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#)
- [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#)
- [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#)
- [Metrics reference for Amazon RDS \(p. 609\)](#)

Overview of monitoring metrics in Amazon RDS

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon RDS and your AWS solutions. To more easily debug multi-point failures, we recommend that you collect monitoring data from all parts of your AWS solution.

Topics

- [Monitoring plan \(p. 511\)](#)
- [Performance baseline \(p. 511\)](#)
- [Performance guidelines \(p. 511\)](#)
- [Monitoring tools \(p. 512\)](#)

Monitoring plan

Before you start monitoring Amazon RDS, create a monitoring plan. This plan should answer the following questions:

- What are your monitoring goals?
- Which resources will you monitor?
- How often will you monitor these resources?
- Which monitoring tools will you use?
- Who will perform the monitoring tasks?
- Whom should be notified when something goes wrong?

Performance baseline

To achieve your monitoring goals, you need to establish a baseline. To do this, measure performance under different load conditions at various times in your Amazon RDS environment. You can monitor metrics such as the following:

- Network throughput
- Client connections
- I/O for read, write, or metadata operations
- Burst credit balances for your DB instances

We recommend that you store historical performance data for Amazon RDS. Using the stored data, you can compare current performance against past trends. You can also distinguish normal performance patterns from anomalies, and devise techniques to address issues.

Performance guidelines

In general, acceptable values for performance metrics depend on what your application is doing relative to your baseline. Investigate consistent or trending variances from your baseline. The following metrics are often the source of performance issues:

- **High CPU or RAM consumption** – High values for CPU or RAM consumption might be appropriate, if they're in keeping with your goals for your application (like throughput or concurrency) and are expected.

- **Disk space consumption** – Investigate disk space consumption if space used is consistently at or above 85 percent of the total disk space. See if it is possible to delete data from the instance or archive data to a different system to free up space.
- **Network traffic** – For network traffic, talk with your system administrator to understand what expected throughput is for your domain network and internet connection. Investigate network traffic if throughput is consistently lower than expected.
- **Database connections** – If you see high numbers of user connections and also decreases in instance performance and response time, consider constraining database connections. The best number of user connections for your DB instance varies based on your instance class and the complexity of the operations being performed. To determine the number of database connections, associate your DB instance with a parameter group where the `User_Connections` parameter is set to a value other than 0 (unlimited). You can either use an existing parameter group or create a new one. For more information, see [Working with parameter groups \(p. 289\)](#).
- **IOPS metrics** – The expected values for IOPS metrics depend on disk specification and server configuration, so use your baseline to know what is typical. Investigate if values are consistently different than your baseline. For best IOPS performance, make sure that your typical working set fits into memory to minimize read and write operations.

When performance falls outside your established baseline, you might need to make changes to optimize your database availability for your workload. For example, you might need to change the instance class of your DB instance. Or you might need to change the number of DB instances and read replicas that are available for clients.

Monitoring tools

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon RDS and your other AWS solutions. AWS provides various monitoring tools to watch Amazon RDS, report when something is wrong, and take automatic actions when appropriate.

Topics

- [Automated monitoring tools \(p. 512\)](#)
- [Manual monitoring tools \(p. 513\)](#)

Automated monitoring tools

We recommend that you automate monitoring tasks as much as possible.

Topics

- [Amazon RDS instance status and recommendations \(p. 512\)](#)
- [Amazon CloudWatch metrics for Amazon RDS \(p. 513\)](#)
- [Amazon RDS Performance Insights and operating-system monitoring \(p. 513\)](#)
- [Integrated services \(p. 513\)](#)

Amazon RDS instance status and recommendations

You can use the following automated tools to watch Amazon RDS and report when something is wrong:

- **Amazon RDS instance status** — View details about the current status of your instance by using the Amazon RDS console, the AWS CLI, or the RDS API.
- **Amazon RDS recommendations** — Respond to automated recommendations for database resources, such as DB instances, read replicas, and DB parameter groups. For more information, see [Viewing Amazon RDS recommendations \(p. 520\)](#).

Amazon CloudWatch metrics for Amazon RDS

Amazon RDS integrates with Amazon CloudWatch for additional monitoring capabilities.

- **Amazon CloudWatch** – This service monitors your AWS resources and the applications you run on AWS in real time. You can use the following Amazon CloudWatch features with Amazon RDS:
 - **Amazon CloudWatch metrics** – Amazon RDS automatically sends metrics to CloudWatch every minute for each active database. You don't get additional charges for Amazon RDS metrics in CloudWatch. For more information, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).
 - **Amazon CloudWatch alarms** – You can watch a single Amazon RDS metric over a specific time period. You can then perform one or more actions based on the value of the metric relative to a threshold that you set. For more information, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).

Amazon RDS Performance Insights and operating-system monitoring

You can use the following automated tools to monitor Amazon RDS performance:

- **Amazon RDS Performance Insights** – Assess the load on your database, and determine when and where to take action. For more information, see [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#).
- **Amazon RDS Enhanced Monitoring** – Look at metrics in real time for the operating system. For more information, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

Integrated services

The following AWS services are integrated with Amazon RDS:

- *Amazon EventBridge* is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. For more information, see [Monitoring Amazon RDS events \(p. 646\)](#).
- *Amazon CloudWatch Logs* lets you monitor, store, and access your log files from Amazon RDS instances, CloudTrail, and other sources. For more information, see [Monitoring Amazon RDS log files \(p. 680\)](#).
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. For more information, see [Monitoring Amazon RDS API calls in AWS CloudTrail \(p. 725\)](#).
- *Database Activity Streams* is an Amazon RDS feature that provides a near-real-time stream of the activity in your Oracle DB instance. For more information, see [Monitoring Amazon RDS for Oracle with Database Activity Streams \(p. 729\)](#).

Manual monitoring tools

You need to manually monitor those items that the CloudWatch alarms don't cover. The Amazon RDS, CloudWatch, AWS Trusted Advisor and other AWS console dashboards provide an at-a-glance view of the state of your AWS environment. We recommend that you also check the log files on your DB instance.

- From the Amazon RDS console, you can monitor the following items for your resources:
 - The number of connections to a DB instance
 - The amount of read and write operations to a DB instance
 - The amount of storage that a DB instance is currently using
 - The amount of memory and CPU being used for a DB instance

- The amount of network traffic to and from a DB instance
- From the Trusted Advisor dashboard, you can review the following cost optimization, security, fault tolerance, and performance improvement checks:
 - Amazon RDS Idle DB Instances
 - Amazon RDS Security Group Access Risk
 - Amazon RDS Backups
 - Amazon RDS Multi-AZ

For more information on these checks, see [Trusted Advisor best practices \(checks\)](#).

- CloudWatch home page shows:
 - Current alarms and status
 - Graphs of alarms and resources
 - Service health status

In addition, you can use CloudWatch to do the following:

- Create [customized dashboards](#) to monitor the services that you care about.
- Graph metric data to troubleshoot issues and discover trends.
- Search and browse all your AWS resource metrics.
- Create and edit alarms to be notified of problems.

Viewing instance status and recommendations

Using the Amazon RDS console, you can quickly access the status of your DB instance and respond to Amazon RDS recommendations.

Topics

- [Viewing Amazon RDS DB instance status \(p. 516\)](#)
- [Viewing Amazon RDS recommendations \(p. 520\)](#)

Viewing Amazon RDS DB instance status

The status of a DB instance indicates the health of the DB instance. You can use the following procedures to view the DB instance status in the Amazon RDS console, the AWS CLI command, or the API operation.

Note

Amazon RDS also uses another status called *maintenance status*, which is shown in the **Maintenance** column of the Amazon RDS console. This value indicates the status of any maintenance patches that need to be applied to a DB instance. Maintenance status is independent of DB instance status. For more information about maintenance status, see [Applying updates for a DB instance \(p. 352\)](#).

Find the possible status values for DB instances in the following table. This table also shows whether you will be billed for the DB instance and storage, billed only for storage, or not billed. For all DB instance statuses, you are always billed for backup usage.

DB instance status	Billed	Description
Available	Billed	The DB instance is healthy and available.
Backing-up	Billed	The DB instance is currently being backed up.
Configuring-enhanced-monitoring	Billed	Enhanced Monitoring is being enabled or disabled for this DB instance.
Configuring-iam-database-auth	Billed	AWS Identity and Access Management (IAM) database authentication is being enabled or disabled for this DB instance.
Configuring-log-exports	Billed	Publishing log files to Amazon CloudWatch Logs is being enabled or disabled for this DB instance.
Converting-to-vpc	Billed	The DB instance is being converted from a DB instance that is not in an Amazon Virtual Private Cloud (Amazon VPC) to a DB instance that is in an Amazon VPC.
Creating	Not billed	The DB instance is being created. The DB instance is inaccessible while it is being created.
Deleting	Not billed	The DB instance is being deleted.
Failed	Not billed	The DB instance has failed and Amazon RDS can't recover it. Perform a point-in-time restore to the latest restorable time of the DB instance to recover the data.
Inaccessible-encryption-credentials	Not billed	The AWS KMS key used to encrypt or decrypt the DB instance can't be accessed or recovered.
Inaccessible-encryption-credentials-recoverable	Billed for storage	The KMS key used to encrypt or decrypt the DB instance can't be accessed. However, if the KMS key is active, restarting the DB instance can recover it. For more information, see Encrypting a DB instance (p. 2001) .
Incompatible-network	Not billed	Amazon RDS is attempting to perform a recovery action on a DB instance but can't do so because the VPC is in a state that prevents the action from being completed. This status can occur if, for example, all available IP addresses in a subnet are in use and Amazon RDS can't get an IP address for the DB instance.

DB instance status	Billed	Description
Incompatible-option-group	Billed	Amazon RDS attempted to apply an option group change but can't do so, and Amazon RDS can't roll back to the previous option group state. For more information, check the Recent Events list for the DB instance. This status can occur if, for example, the option group contains an option such as TDE and the DB instance doesn't contain encrypted information.
Incompatible-parameters	Billed	Amazon RDS can't start the DB instance because the parameters specified in the DB instance's DB parameter group aren't compatible with the DB instance. Revert the parameter changes or make them compatible with the DB instance to regain access to your DB instance. For more information about the incompatible parameters, check the Recent Events list for the DB instance.
Incompatible-restore	Not billed	Amazon RDS can't do a point-in-time restore. Common causes for this status include using temp tables, using MyISAM tables with MySQL, or using Aria tables with MariaDB.
Insufficient-capacity	Not billed	Amazon RDS can't create your instance because sufficient capacity isn't currently available. To create your DB instance in the same AZ with the same instance type, delete your DB instance, wait a few hours, and try to create again. Alternatively, create a new instance using a different instance class or AZ.
Maintenance	Billed	Amazon RDS is applying a maintenance update to the DB instance. This status is used for instance-level maintenance that RDS schedules well in advance.
Modifying	Billed	The DB instance is being modified because of a customer request to modify the DB instance.
Moving-to-vpc	Billed	The DB instance is being moved to a new Amazon Virtual Private Cloud (Amazon VPC).
Rebooting	Billed	The DB instance is being rebooted because of a customer request or an Amazon RDS process that requires the rebooting of the DB instance.
Resetting-master-credentials	Billed	The master credentials for the DB instance are being reset because of a customer request to reset them.
Renaming	Billed	The DB instance is being renamed because of a customer request to rename it.
Restore-error	Billed	The DB instance encountered an error attempting to restore to a point-in-time or from a snapshot.
Starting	Billed for storage	The DB instance is starting.
Stopped	Billed for storage	The DB instance is stopped.

DB instance status	Billed	Description
Stopping	Billed for storage	The DB instance is being stopped.
Storage-full	Billed	The DB instance has reached its storage capacity allocation. This is a critical status, and we recommend that you fix this issue immediately. To do so, scale up your storage by modifying the DB instance. To avoid this situation, set Amazon CloudWatch alarms to warn you when storage space is getting low.
Storage-optimization	Billed	Amazon RDS is optimizing the storage of your DB instance. The DB instance is fully operational. The storage optimization process is usually short, but can sometimes take up to and even beyond 24 hours.
Upgrading	Billed	The database engine version is being upgraded.

Console

To view the status of a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

The **Databases page** appears with the list of DB instances. For each DB instance , the status value is displayed.

Databases			
<input type="text"/> Filter by databases			
DB identifier	Role	Status	
database-1	Instance	Stopped	
database-2	Instance	Creating	
database-3	Instance	Available	
database-4	Instance	Configuring-enhanced-monitoring	
database-5	Instance		

CLI

To view DB instance and its status information by using the AWS CLI, use the [describe-db-instances](#) command. For example, the following AWS CLI command lists all the DB instances information .

```
aws rds describe-db-instances
```

To view a specific DB instance and its status, call the [describe-db-instances](#) command with the following option:

- **DBInstanceIdentifier** – The name of the DB instance.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

To view just the status of all the DB instances, use the following query in AWS CLI.

```
aws rds describe-db-instances --query 'DBInstances[*].  
[DBInstanceIdentifier,DBInstanceStatus]' --output table
```

API

To view the status of the DB instance using the Amazon RDS API, call the [DescribeDBInstances](#) operation.

Viewing Amazon RDS recommendations

Amazon RDS provides automated recommendations for database resources, such as DB instances, read replicas, and DB parameter groups. These recommendations provide best practice guidance by analyzing DB instance configuration, usage, and performance data.

You can find examples of these recommendations in the following table.

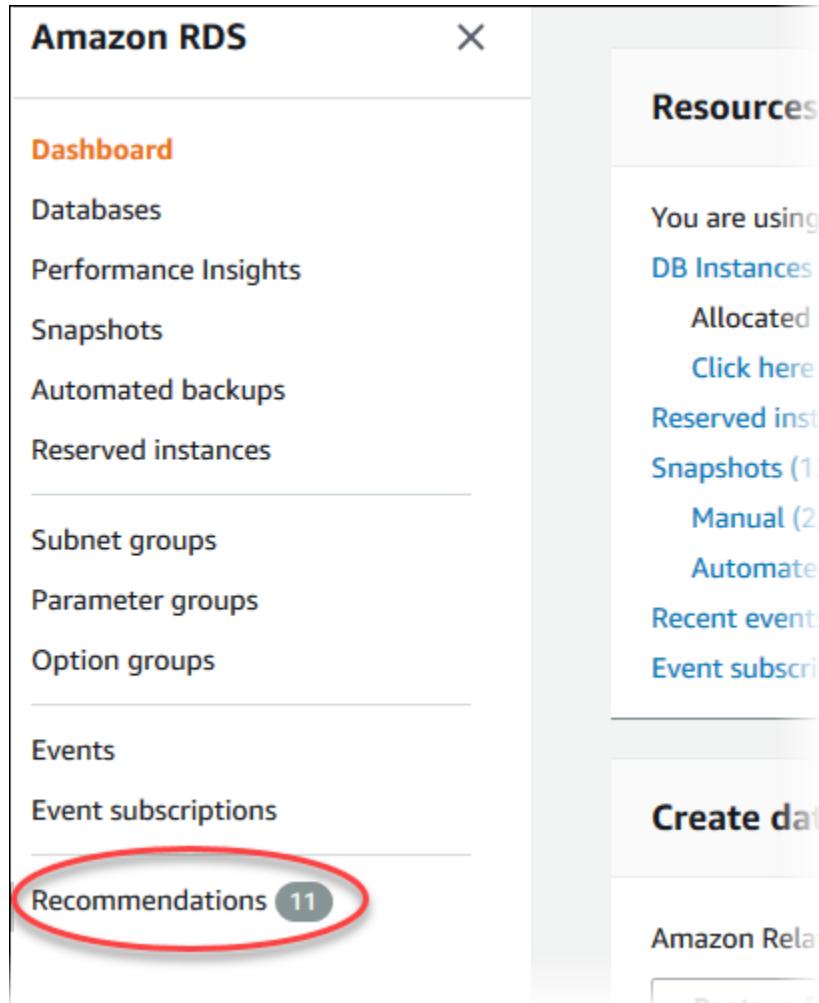
Type	Description	Recommendation	Additional information
Engine version outdated	Your DB instance is not running the latest minor engine version.	We recommend that you upgrade to the latest version because it contains the latest security fixes and other improvements.	Upgrading a DB instance engine version (p. 360)
Pending maintenance available	You have pending maintenance available on your DB instance.	We recommend that you perform the pending maintenance available on your DB instance. Updates to the operating system most often occur for security issues and should be done as soon as possible.	Maintaining a DB instance (p. 350)
Automated backups disabled	Your DB instance has automated backups disabled.	We recommend that you enable automated backups on your DB instance. Automated backups enable point-in-time recovery of your DB instance. You receive backup storage up to the storage size of your DB instance at no additional charge.	Working with backups (p. 427)
Magnetic volumes in use	Your DB instance is using magnetic storage.	Magnetic storage is not recommended for most DB instances. We recommend switching to General Purpose (SSD) storage or provisioned IOPS storage.	Amazon RDS DB instance storage (p. 64)
Enhanced Monitoring disabled	Your DB instance doesn't have Enhanced Monitoring enabled.	We recommend enabling Enhanced Monitoring. Enhanced Monitoring provides real-time operating system metrics for monitoring and troubleshooting.	Monitoring OS metrics with Enhanced Monitoring (p. 600)
Encryption disabled	Your DB instance doesn't have encryption enabled.	We recommend enabling encryption. You can encrypt your existing Amazon RDS DB instances by restoring from an encrypted snapshot.	Encrypting Amazon RDS resources (p. 2000)
Previous generation DB instance class in use	Your DB instance is running on a previous-generation DB instance class.	Previous-generation DB instance classes have been replaced by DB instance classes with better price, better performance, or both. We recommend running your DB instance on a later generation DB instance class.	DB instance classes (p. 10)
Huge pages not used for	The use_large_pages	For increased database scalability, we recommend setting	Turning on HugePages for an

Type	Description	Recommendation	Additional information
an Oracle DB instance	parameter is not set to ONLY in the DB parameter group used by your DB instance.	use_large_pages to ONLY in the DB parameter group used by your DB instance.	RDS for Oracle instance (p. 1610)
Nondefault custom memory parameters	Your DB parameter group sets memory parameters that diverge too much from the default values.	Settings that diverge too much from the default values can cause poor performance and errors. We recommend setting custom memory parameters to their default values in the DB parameter group used by the DB instance.	Working with parameter groups (p. 289)
Change buffering enabled for a MySQL DB instance	Your DB parameter group has change buffering enabled.	Change buffering allows a MySQL DB instance to defer some writes necessary to maintain secondary indexes. This configuration can improve performance slightly, but it can create a large delay in crash recovery. During crash recovery, the secondary index must be brought up to date. So, the benefits of change buffering are outweighed by the potentially very long crash recovery events. We recommend disabling change buffering.	Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance on the AWS Database Blog
Query cache enabled for a MySQL DB instance	Your DB parameter group has query cache parameter enabled.	The query cache can cause the DB instance to appear to stall when changes require the cache to be purged. Most workloads don't benefit from a query cache. The query cache was removed from MySQL version 8.0. We recommend that you disable the query cache parameter.	Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance on the AWS Database Blog
Logging to table	Your DB parameter group sets logging output to TABLE.	Setting logging output to TABLE uses more storage than setting this parameter to FILE. To avoid reaching the storage limit, we recommend setting the logging output parameter to FILE.	MySQL database log files (p. 700)

Amazon RDS generates recommendations for a resource when the resource is created or modified. Amazon RDS also periodically scans your resources and generates recommendations.

To view Amazon RDS recommendations

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Recommendations**.



The Recommendations page appears.

This screenshot shows the 'Recommendations' page. At the top, there are tabs for Active (2), Dismissed (0), Scheduled (0), and Applied (1). Below the tabs, there are two items listed under the 'Active' tab:

- ▶ Engine version outdated for DB instances (1)
DB instances that are not running the latest minor engine version. [Info](#)
- ▶ Enhanced monitoring disabled (1)
DB instances that don't have Enhanced Monitoring enabled. [Info](#)

3. On the **Recommendations** page, choose one of the following:

- **Active** – Shows the current recommendations that you can apply, dismiss, or schedule.
- **Dismissed** – Shows the recommendations that have been dismissed. When you choose **Dismissed**, you can apply these dismissed recommendations.
- **Scheduled** – Shows the recommendations that are scheduled but not yet applied. These recommendations will be applied in the next scheduled maintenance window.
- **Applied** – Shows the recommendations that are currently applied.

From any list of recommendations, you can open a section to view the recommendations in that section.

Recommendations

Active (2) Dismissed (0) Scheduled (0) Applied (1)

▼ Engine version outdated for DB instances (1)
DB instances that are not running the latest minor engine version. [Info](#)

DB instances

<input type="checkbox"/>	Resource	Recommendation	Re
<input type="checkbox"/>	database-1	Your DB instance is running mysql version 5.6.34. We recommend that you upgrade to version 5.6.41 because it contains the latest security fixes and other improvements.	Th (P)

▶ Enhanced monitoring disabled (1)
DB instances that don't have Enhanced Monitoring enabled. [Info](#)

To configure preferences for displaying recommendations in each section, choose the **Preferences** icon.

Recommendations

Active (2) Dismissed (0) Scheduled (0) Applied (1)

▼ Engine version outdated for DB instances (1)
DB instances that are not running the latest minor engine version. [Info](#)

DB instances

<input type="checkbox"/>	Resource	Recommendation	Re
<input type="checkbox"/>	database-1	Your DB instance is running mysql version 5.6.34. We recommend that you upgrade to version 5.6.41 because it contains the latest security fixes and other improvements.	Th (P)

▶ Enhanced monitoring disabled (1)
DB instances that don't have Enhanced Monitoring enabled. [Info](#)

From the **Preferences** window that appears, you can set display options. These options include the visible columns and the number of recommendations to display on the page.

4. (optional) Respond to your active recommendations as follows:
 - a. Choose **Active** and open one or more sections to view the recommendations in them.
 - b. Choose one or more recommendations and choose **Apply now** (to apply them immediately), **Schedule** (to apply them in next maintenance window), or **Dismiss**.

If the **Apply now** button appears for a recommendation but is unavailable (grayed out), the DB instance is not available. You can apply recommendations immediately only if the DB instance

status is **available**. For example, you can't apply recommendations immediately to the DB instance if its status is **modifying**. In this case, wait for the DB instance to be available and then apply the recommendation.

If the **Apply now** button doesn't appear for a recommendation, you can't apply the recommendation using the **Recommendations** page. You can modify the DB instance to apply the recommendation manually.

For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

When you choose **Apply now**, a brief DB instance outage might result.

Viewing metrics in the Amazon RDS console

Amazon RDS integrates with Amazon CloudWatch to display a variety of RDS DB instance metrics in the RDS console. For descriptions of these metrics, see [Metrics reference for Amazon RDS \(p. 609\)](#).

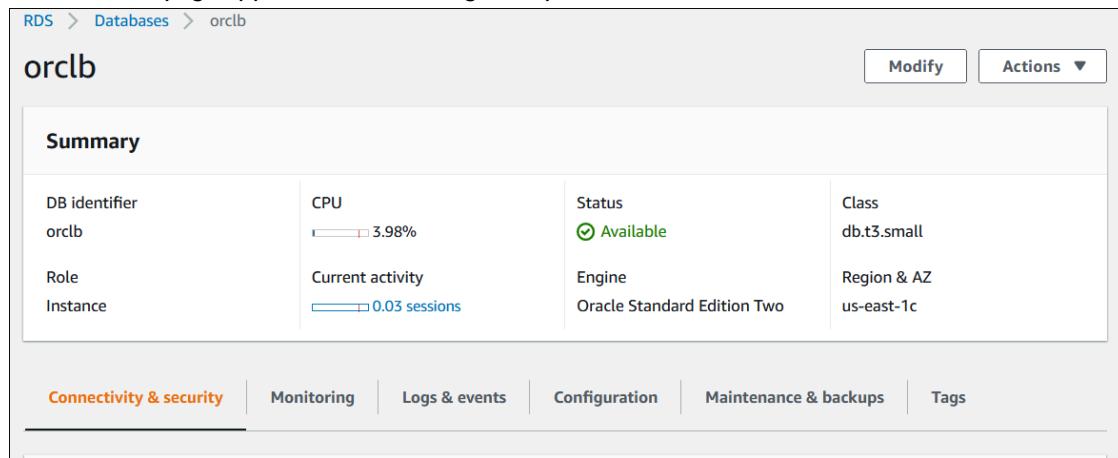
The **Monitoring** tab for your RDS DB instance shows the following categories of metrics:

- **CloudWatch** – Shows the Amazon CloudWatch metrics for that you can access in the RDS console. You can also access these metrics in the CloudWatch console. Each metric includes a graph that shows the metric monitored over a specific time span. For a list of CloudWatch metrics, see [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).
- **Enhanced monitoring** – Shows a summary of operating-system metrics when your RDS DB instance has turned on Enhanced Monitoring. RDS delivers the metrics from Enhanced Monitoring to your Amazon CloudWatch Logs account. Each OS metric includes a graph showing the metric monitored over a specific time span. For an overview, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#). For a list of Enhanced Monitoring metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#).
- **OS Process list** – Shows details for each process running in your DB instance.
- **Performance Insights** – Opens the Amazon RDS Performance Insights dashboard for a DB instance. For an overview of Performance Insights, see [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#). For a list of Performance Insights metrics, see [Amazon CloudWatch metrics for Performance Insights \(p. 617\)](#).

To view metrics for your DB instance in the RDS console

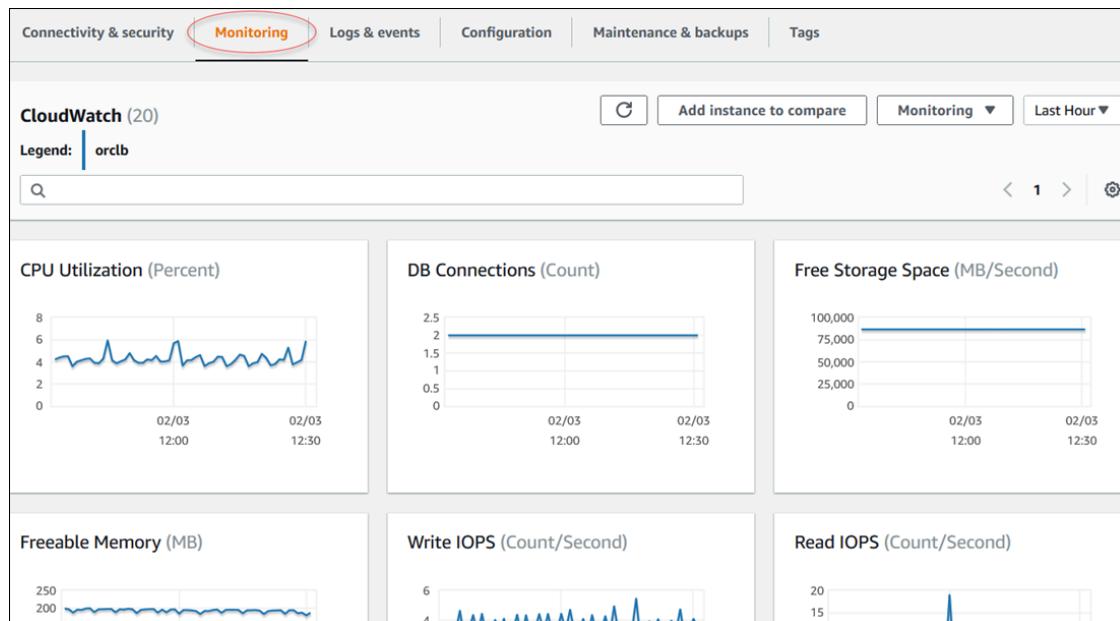
1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that you want to monitor.

The database page appears. The following example shows an Oracle database named orclb.

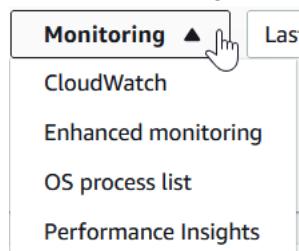


4. Scroll down and choose **Monitoring**.

The monitoring section appears. By default, CloudWatch metrics are shown. For descriptions of these metrics, see [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).

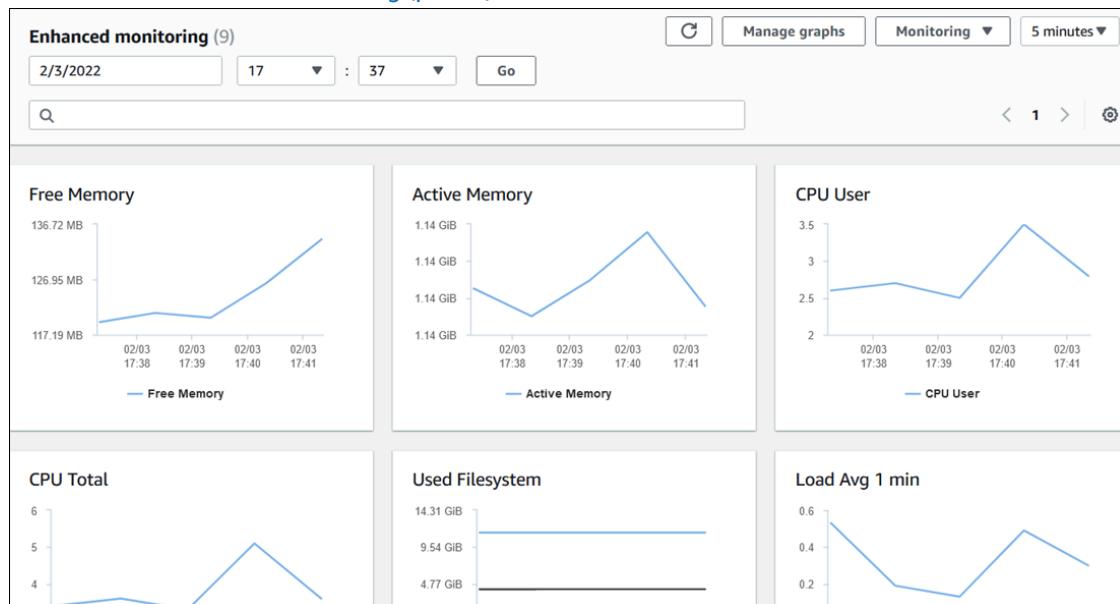


- Choose **Monitoring** to see the metric categories.



- Choose the category of metrics that you want to see.

The following example shows Enhanced Monitoring metrics. For descriptions of these metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#).



Tip

To choose the time range of the metrics represented by the graphs, you can use the time range list.

To bring up a more detailed view, you can choose any graph. You can also apply metric-specific filters to the data.

Monitoring Amazon RDS metrics with Amazon CloudWatch

Amazon CloudWatch is a metrics repository. The repository collects and processes raw data from Amazon RDS into readable, near real-time metrics. For a complete list of Amazon RDS metrics sent to CloudWatch, see [Metrics reference for Amazon RDS](#).

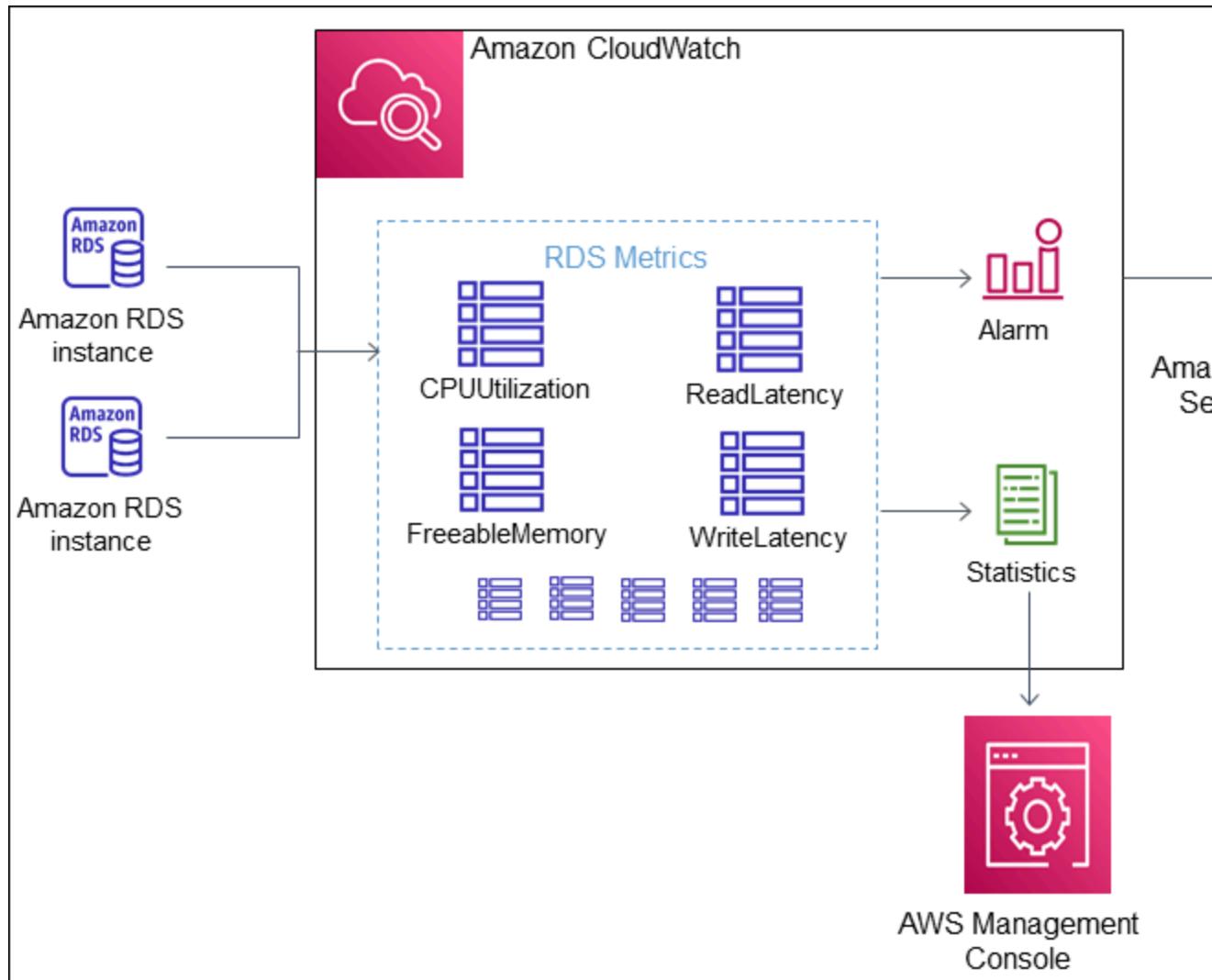
Topics

- [Overview of Amazon RDS and Amazon CloudWatch \(p. 529\)](#)
- [Viewing DB instance metrics in the CloudWatch console and AWS CLI \(p. 530\)](#)
- [Creating CloudWatch alarms to monitor Amazon RDS \(p. 535\)](#)
- [Tutorial: Creating an Amazon CloudWatch alarm for Multi-AZ DB cluster replica lag \(p. 536\)](#)

Overview of Amazon RDS and Amazon CloudWatch

By default, Amazon RDS automatically sends metric data to CloudWatch in 1-minute periods. For example, the CPUUtilization metric records the percentage of CPU utilization for a DB instance over time. Data points with a period of 60 seconds (1 minute) are available for 15 days. This means that you can access historical information and see how your web application or service is performing.

As shown in the following diagram, you can set up alarms for your CloudWatch metrics. For example, you might create an alarm that signals when the CPU utilization for an instance is over 70%. You can configure Amazon Simple Notification Service to email you when the threshold is passed.



Amazon RDS publishes the following types of metrics to Amazon CloudWatch:

- Metrics for your RDS DB instances

For a table of these metrics, see [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).

- Performance Insights metrics

For a table of these metrics, see [Amazon CloudWatch metrics for Performance Insights \(p. 617\)](#) and [Performance Insights counter metrics \(p. 618\)](#).

- Enhanced Monitoring metrics (published to Amazon CloudWatch Logs)

For a table of these metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#).

- Usage metrics for the Amazon RDS service quotas in your AWS account

For a table of these metrics, see [Amazon CloudWatch usage metrics for Amazon RDS \(p. 615\)](#). For more information about Amazon RDS quotas, see [Quotas and constraints for Amazon RDS \(p. 2135\)](#).

For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the *Amazon CloudWatch User Guide*. For more information about CloudWatch metrics retention, see [Metrics retention](#).

Viewing DB instance metrics in the CloudWatch console and AWS CLI

Following, you can find details about how to view metrics for your DB instance using CloudWatch. For information on monitoring metrics for your DB instance's operating system in real time using CloudWatch Logs, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

When you use Amazon RDS resources, Amazon RDS sends metrics and dimensions to Amazon CloudWatch every minute. You can use the following procedures to view the metrics for Amazon RDS in the CloudWatch console and CLI.

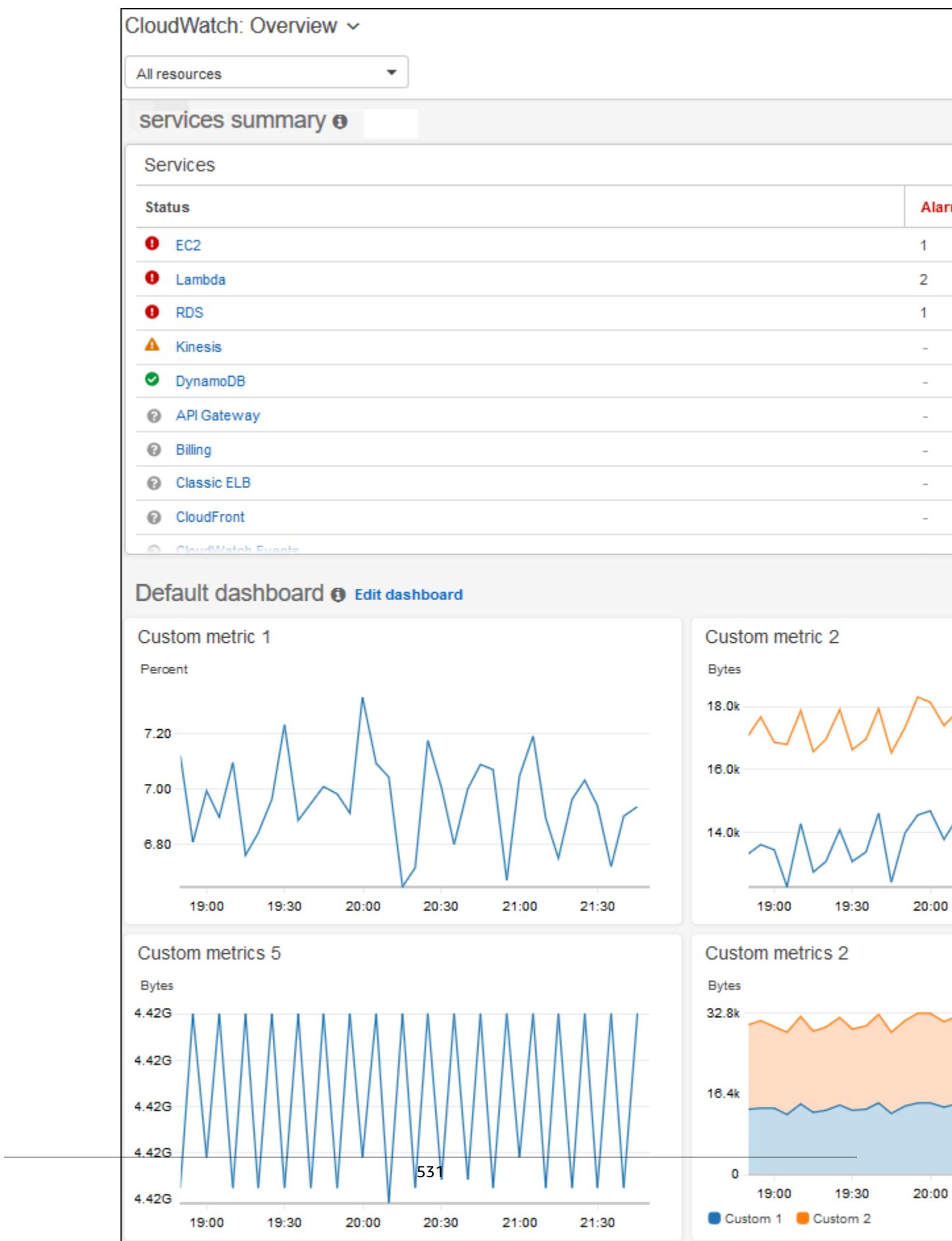
Console

To view metrics using the Amazon CloudWatch console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

The CloudWatch overview home page appears.



2. If necessary, change the AWS Region. From the navigation bar, choose the AWS Region where your AWS resources are. For more information, see [Regions and endpoints](#).
3. In the navigation pane, choose **Metrics** and then **All metrics**.

The screenshot shows the 'All metrics' view in the CloudWatch Metrics console. At the top, there are tabs: 'Browse' (which is selected), 'Query', 'Graphed metrics', 'Options', 'Source', and 'Add math'. Below the tabs, it says 'Metrics (1301)' and has a 'Graph with SQL' button. A search bar says 'Search for any metric, dimension or resource id' with a dropdown set to 'N. Virginia'. There are several cards representing different metric namespaces: EBS (9), EC2 (17), Events, Lambda (26), Logs (35), RDS (circled in red), S3 (8), SSM Run Command (3), and Usage.

4. Scroll down and choose the **RDS** metric namespace.

The page displays the Amazon RDS dimensions. For descriptions of these dimensions, see [Amazon CloudWatch dimensions for Amazon RDS \(p. 616\)](#).

The screenshot shows the 'RDS' metric namespace view. At the top, there are tabs: 'Browse' (selected), 'Query', 'Graphed metrics', 'Options', 'Source', and 'Add math'. Below the tabs, it says 'Metrics (1152)' and has a 'Graph with SQL' button. A search bar says 'Search for any metric, dimension or resource id' with a dropdown set to 'N. Virginia'. The path 'All > RDS' is shown. There are several cards representing dimensions: DBClusterIdentifier, Role (153), DbClusterIdentifier, EngineName (6), Per-Database Metrics (332), By Database Class (191), Across All Databases (114), and By Database Engine.

5. Choose a metric dimension, for example **By Database Class**.

Browse Query Graphed metrics (1) Options Source Add math ▾ Add query ▾

Metrics (191) [Info](#)

N. Virginia ▾ All > RDS > By Database Class Search for any metric, dimension or resource id

	Metric name
<input type="checkbox"/>	DatabaseClass (191)
<input type="checkbox"/>	db.r6g.large ▾
<input type="checkbox"/>	db.r6g.large ▾
<input type="checkbox"/>	db.r6g.large ▾

6. Do any of the following actions:

- To sort the metrics, use the column heading.
- To graph a metric, select the check box next to the metric.
- To filter by resource, choose the resource ID, and then choose **Add to search**.
- To filter by metric, choose the metric name, and then choose **Add to search**.

The following example filters on the **db.t3.medium** class and graphs the **CPUUtilization** metric.

Untitled graph [Edit](#)

Browse Query Graphed metrics (2/3) Options Source Add math ▾ Add query ▾

Metrics (17) [Info](#)

N. Virginia ▾ All > RDS > By Database Class

CPU [Edit](#) [X](#)

	Metric name
<input type="checkbox"/>	DatabaseClass (17)
<input type="checkbox"/>	db.t3.medium ▾
<input checked="" type="checkbox"/>	db.t3.medium ▾
<input type="checkbox"/>	db.t3.medium ▾

Add to search
 Search for this only
 Remove from graph
 Graph this metric only
 Graph all search results
 Graph with SQL query
 What is this? [Edit](#)

AWS CLI

To obtain metric information by using the AWS CLI, use the CloudWatch command [list-metrics](#). In the following example, you list all metrics in the AWS/RDS namespace.

```
aws cloudwatch list-metrics --namespace AWS/RDS
```

To obtain metric statistics, use the command [get-metric-statistics](#). The following command gets CPUUtilization statistics for instance *my-instance* over the specific 24-hour period, with a 5-minute granularity.

Example

For Linux, macOS, or Unix:

```
aws cloudwatch get-metric-statistics --namespace AWS/RDS \
    --metric-name CPUUtilization \
    --start-time 2021-12-15T00:00:00Z \
    --end-time 2021-12-16T00:00:00Z \
    --period 360 \
    --statistics Minimum \
    --dimensions Name=DBInstanceIdentifier,Value=my-instance
```

For Windows:

```
aws cloudwatch get-metric-statistics --namespace AWS/RDS ^
    --metric-name CPUUtilization ^
    --start-time 2021-12-15T00:00:00Z ^
    --end-time 2021-12-16T00:00:00Z ^
    --period 360 ^
    --statistics Minimum ^
    --dimensions Name=DBInstanceIdentifier,Value=my-instance
```

Sample output appears as follows:

```
{
  "Datapoints": [
    {
      "Timestamp": "2021-12-15T18:00:00Z",
      "Minimum": 8.7,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2021-12-15T23:54:00Z",
      "Minimum": 8.12486458559024,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2021-12-15T17:24:00Z",
      "Minimum": 8.841666666666667,
      "Unit": "Percent"
    },
    ...
    {
      "Timestamp": "2021-12-15T22:48:00Z",
      "Minimum": 8.366248354248954,
      "Unit": "Percent"
    }
  ],
  "Label": "CPUUtilization"
```

}

For more information, see [Getting statistics for a metric](#) in the *Amazon CloudWatch User Guide*.

Creating CloudWatch alarms to monitor Amazon RDS

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period that you specify. The alarm can also perform one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or Amazon EC2 Auto Scaling policy.

Alarms invoke actions for sustained state changes only. CloudWatch alarms don't invoke actions simply because they are in a particular state. The state must have changed and have been maintained for a specified number of time periods. The following procedures show how to create alarms for Amazon RDS.

To set alarms using the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. Choose **Alarms, All alarms**.

Choose **Create an alarm**.

This action launches a wizard.

3. Choose **Select metric**.

4. In **Browse**, choose **RDS**.

5. Search for the metric that you want to place an alarm on. For example, search for **CPUUtilization**. To display only Amazon RDS metrics, search for the identifier of your resource.

6. Choose the metric to create an alarm on. Then choose **Select metric**.

7. In **Conditions**, define the alarm condition. Then choose **Next**.

For example, you can specify that the alarm should be set when CPU utilization is over 75%.

8. Choose your notification method. Then choose **Next**.

For example, to configure CloudWatch to send you an email when the alarm state is reached, do the following:

1. Choose **Create new topic** (if one doesn't exist).

2. Enter a topic name.

3. Enter the email endpoints.

The email addresses must be verified before they receive notifications. Emails are only sent when the alarm enters an alarm state. If this alarm state change happens before the email addresses are verified, the addresses don't receive a notification.

4. Choose **Create topic**.

5. Choose **Next**.

9. Enter a name and description for the alarm. The name must contain only ASCII characters. Then choose **Next**.

10. Preview the alarm that you're about to create. Then choose **Create alarm**.

To set an alarm using the AWS CLI

- Call [put-metric-alarm](#). For more information, see [AWS CLI Command Reference](#).

To set an alarm using the CloudWatch API

- Call [PutMetricAlarm](#). For more information, see [Amazon CloudWatch API Reference](#)

For more information about setting up Amazon SNS topics and creating alarms, see [Using Amazon CloudWatch alarms](#).

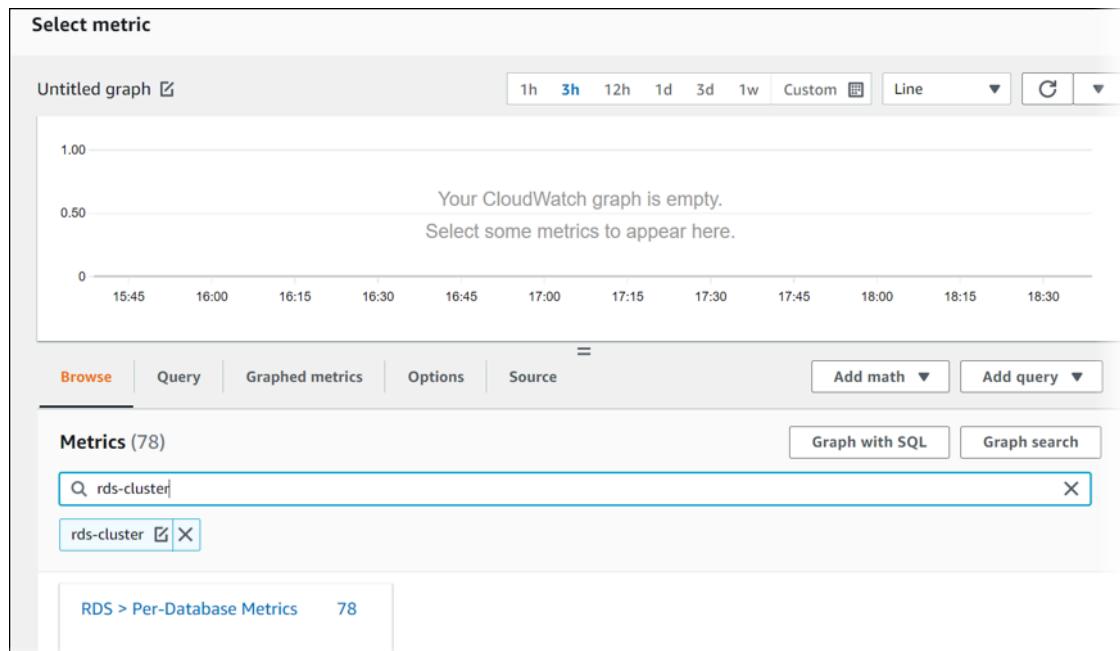
Tutorial: Creating an Amazon CloudWatch alarm for Multi-AZ DB cluster replica lag

You can create an Amazon CloudWatch alarm that sends an Amazon SNS message when replica lag for a Multi-AZ DB cluster has exceeded a threshold. An alarm watches the `ReplicaLag` metric over a time period that you specify. The action is a notification sent to an Amazon SNS topic or Amazon EC2 Auto Scaling policy.

To set a CloudWatch alarm for Multi-AZ DB cluster replica lag

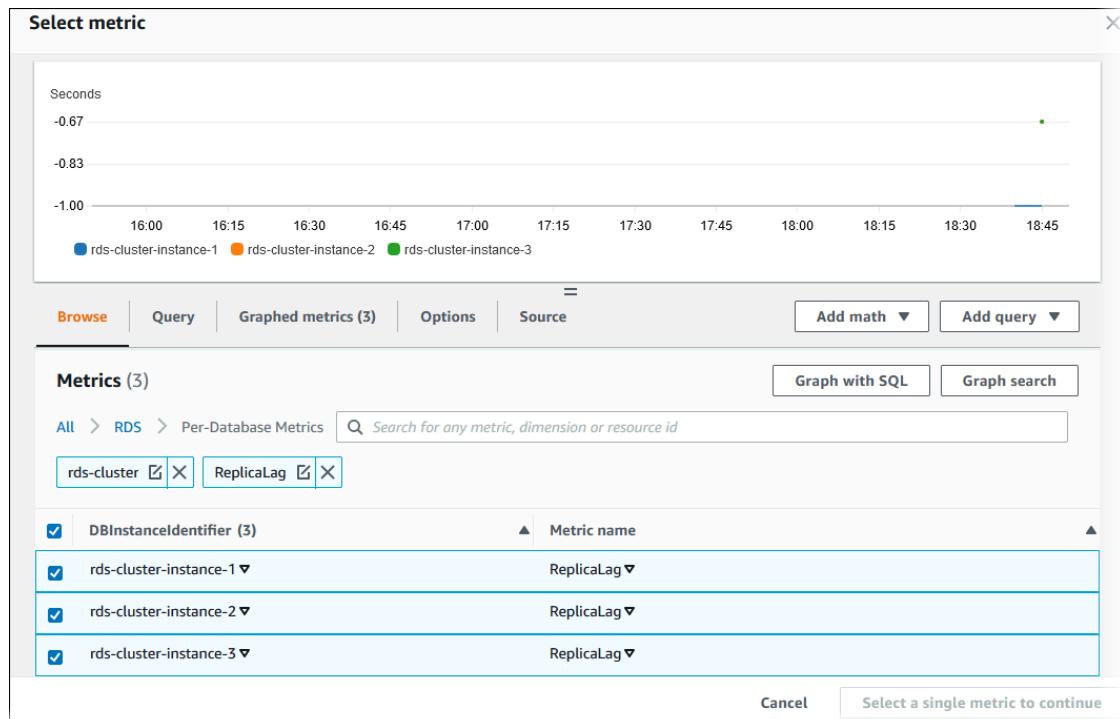
- Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
- In the navigation pane, choose **Alarms, All alarms**.
- Choose **Create alarm**.
- On the **Specify metric and conditions** page, choose **Select metric**.
- In the search box, enter the name of your Multi-AZ DB cluster and press Enter.

The following image shows the **Select metric** page with a Multi-AZ DB cluster named `rds-cluster` entered.



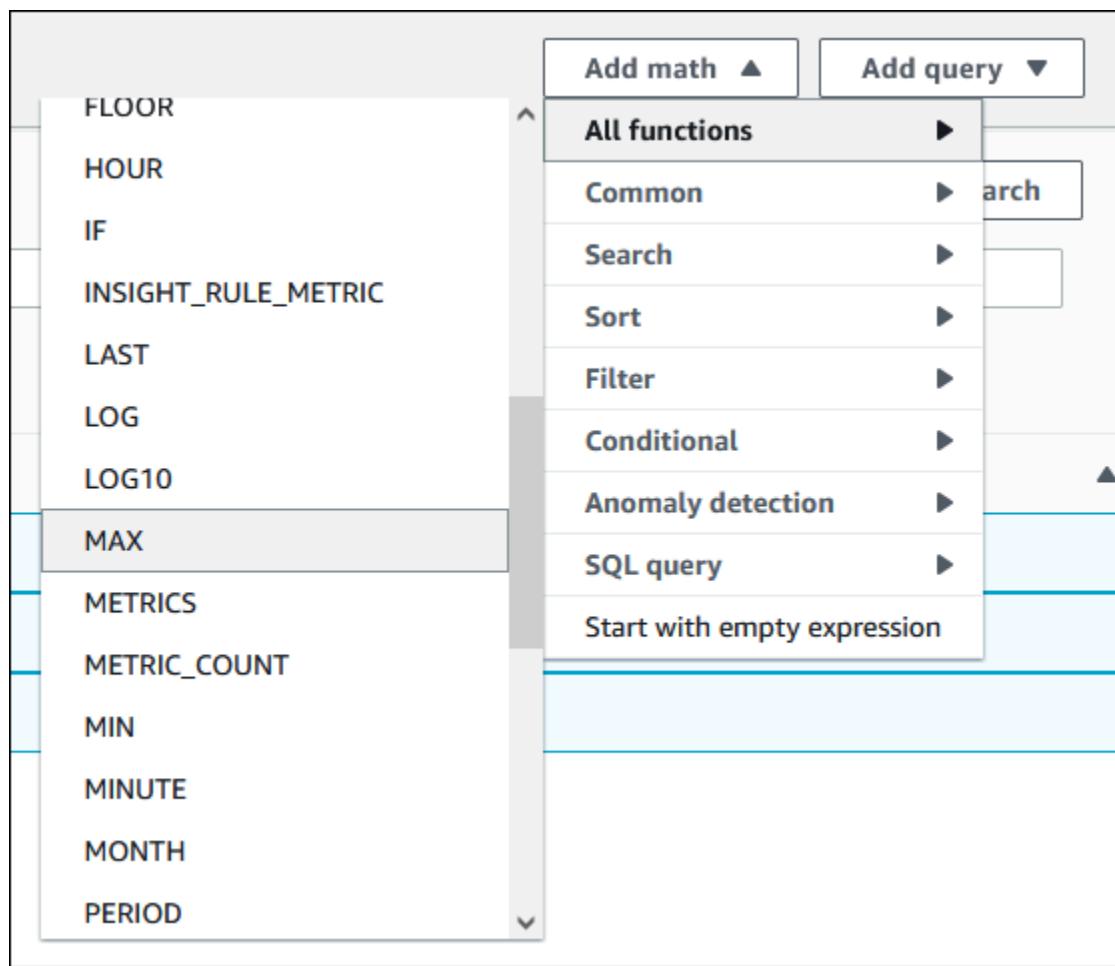
- Choose **RDS, Per-Database Metrics**.
- In the search box, enter **ReplicaLag** and press Enter, then select each DB instance in the DB cluster.

The following image shows the **Select metric** page with the DB instances selected for the `ReplicaLag` metric.



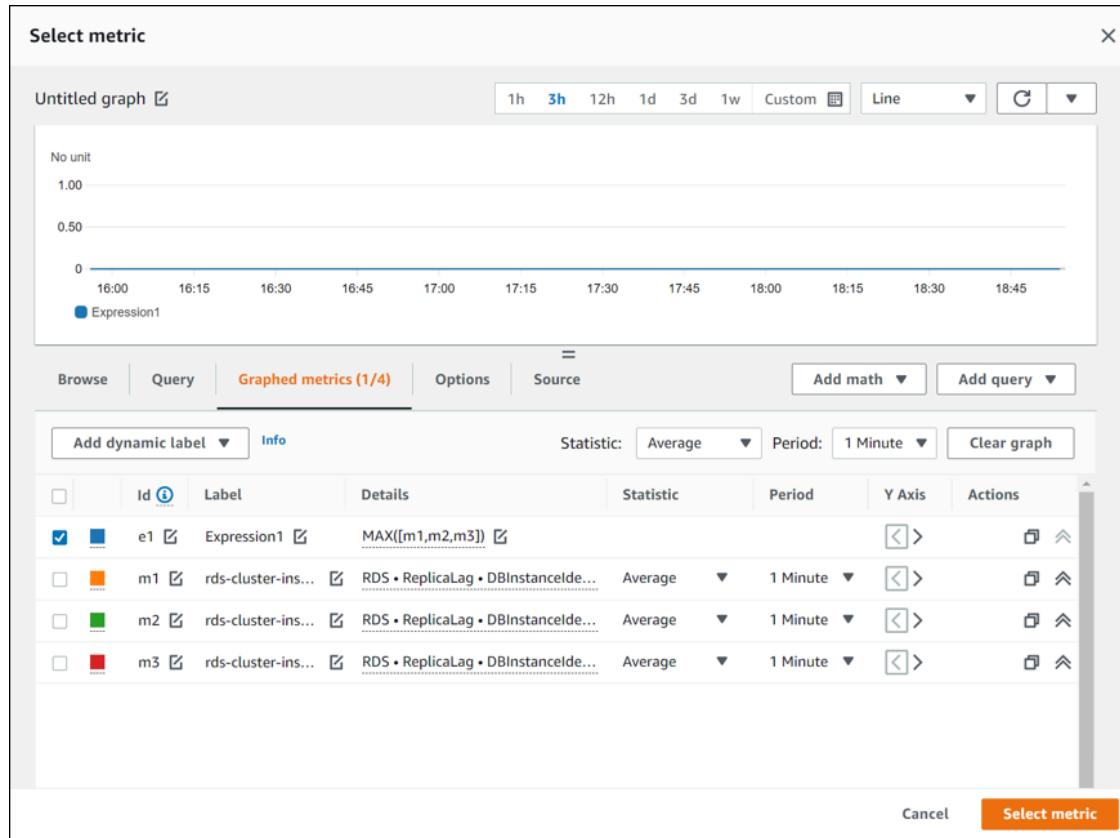
This alarm considers the replica lag for all three of the DB instances in the Multi-AZ DB cluster. The alarm responds when any DB instance exceeds the threshold. It uses a math expression that returns the maximum value of the three metrics. Start by sorting by metric name, and then choose all three **ReplicaLag** metrics.

8. From Add math, choose All functions, MAX.



9. Choose the **Graphed metrics** tab, and edit the details for **Expression1** to **MAX([m1,m2,m3])**.
10. For all three **ReplicaLag** metrics, change the **Period** to **1 minute**.
11. Clear selection from all metrics except for **Expression1**.

The **Select metric** page should look similar to the following image.



12. Choose **Select metric**.
13. On the **Specify metric and conditions** page, change the label to a meaningful name, such as **ClusterReplicaLag**, and enter a number of seconds in **Define the threshold value**. For this tutorial, enter **1200** seconds (20 minutes). You can adjust this value for your workload requirements.

The **Specify metric and conditions** page should look similar to the following image.

Specify metric and conditions

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

No unit

1,000

500

0

17:00 18:00 19:00

ClusterReplicaLag

Label

ClusterReplicaLag

Math expression

MAX([m1,m2,m3])

Metrics

m1 | AWS/RDS | ReplicaLag | DBInstanceIdentifier : ...
m2 | AWS/RDS | ReplicaLag | DBInstanceIdentifier : ...
m3 | AWS/RDS | ReplicaLag | DBInstanceIdentifier : ...

Period

1 minute

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever ClusterReplicaLag is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

than...

Define the threshold value.

1200

Must be a number

► Additional configuration

Cancel

Next

14. Choose **Next**, and the **Configure actions** page appears.
15. Keep **In alarm** selected, choose **Create new topic**, and enter the topic name and a valid email address.

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN

Create a new topic...
The topic name must be unique.

Cluster-ReplicaLag-Notification

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

user1@example.com

user1@example.com, user2@example.com

Create topic

Add notification

16. Choose **Create topic**, and then choose **Next**.
17. On the **Add name and description** page, enter the **Alarm name** and **Alarm description**, and then choose **Next**.

Add name and description

Name and description

Alarm name
Multi-AZ DB cluster replica lag

Alarm description - *optional*
Alarm due to excessive replica lag on a Multi-AZ DB cluster

Up to 1024 characters (59/1024)

[Cancel](#) [Previous](#) [Next](#)

18. Preview the alarm that you're about to create on the [Preview and create](#) page, and then choose [Create alarm](#).

Monitoring DB load with Performance Insights on Amazon RDS

Performance Insights expands on existing Amazon RDS monitoring features to illustrate and help you analyze your database performance. With the Performance Insights dashboard, you can visualize the database load on your Amazon RDS DB instance load and filter the load by waits, SQL statements, hosts, or users. For information about using Performance Insights with Amazon DocumentDB, see [Amazon DocumentDB Developer Guide](#).

Topics

- [Overview of Performance Insights on Amazon RDS \(p. 543\)](#)
- [Turning Performance Insights on and off \(p. 549\)](#)
- [Turning on the Performance Schema for Performance Insights on Amazon RDS for MariaDB or MySQL \(p. 553\)](#)
- [Configuring access policies for Performance Insights \(p. 556\)](#)
- [Analyzing metrics with the Performance Insights dashboard \(p. 559\)](#)
- [Retrieving metrics with the Performance Insights API \(p. 584\)](#)
- [Logging Performance Insights calls using AWS CloudTrail \(p. 598\)](#)

Overview of Performance Insights on Amazon RDS

By default, Performance Insights is turned on in the console create wizard for all Amazon RDS engines. If you have more than one database on a DB instance, Performance Insights aggregates performance data.

You can find an overview of Performance Insights for Amazon RDS in the following video.

Using Performance Insights to Analyze Performance of Amazon Aurora PostgreSQL

Important

The following topics describe using Amazon RDS Performance Insights with non-Aurora DB engines. For information about using Amazon RDS Performance Insights with Amazon Aurora, see [Using Amazon RDS Performance Insights](#) in the [Amazon Aurora User Guide](#).

Topics

- [Database load \(p. 543\)](#)
- [Maximum CPU \(p. 547\)](#)
- [Amazon RDS DB engine, Region, and instance class support for Performance Insights \(p. 547\)](#)
- [Pricing and data retention for Performance Insights \(p. 548\)](#)

Database load

Database load (DB load) measures the level of activity in your database. The key metric in Performance Insights is DBLoad, which is collected every second.

Topics

- [Active sessions \(p. 544\)](#)
- [Average active sessions \(p. 544\)](#)
- [Average active executions \(p. 544\)](#)
- [Dimensions \(p. 545\)](#)

Active sessions

A *database session* represents an application's dialogue with a relational database. An *active session* is a connection that has submitted work to the DB engine and is waiting for a response.

A session is active when it's either running on CPU or waiting for a resource to become available so that it can proceed. For example, an active session might wait for a page to be read into memory, and then consume CPU while it reads data from the page.

Average active sessions

The *average active sessions (AAS)* is the unit for the DBLoad metric in Performance Insights. To get the average active sessions, Performance Insights samples the number of sessions concurrently running a query. The AAS is the total number of sessions divided by the total number of samples for a specific time period. The following table shows 5 consecutive samples of a running query.

Sample	Number of sessions running query	AAS	Calculation
1	2	2	2 sessions / 1 sample
2	0	1	2 sessions / 2 samples
3	4	2	6 sessions / 3 samples
4	0	1.5	6 sessions / 4 samples
5	4	2	10 sessions / 5 samples

In the preceding example, the DB load for the time interval was 2 AAS. This measurement means that, on average, 2 sessions were active at a time during the time period when the 5 samples were taken.

An analogy for DB load is activity in a warehouse. Suppose that the warehouse employs 100 workers. If 1 order comes in, 1 worker fulfills the order while the other workers are idle. If 100 orders come in, all 100 workers fulfill orders simultaneously. If you periodically sample how many workers are active over a given time period, you can calculate the average number of active workers. The calculation shows that, on average, N workers are busy fulfilling orders at any given time. If the average was 50 workers yesterday and 75 workers today, the activity level in the warehouse increased. In the same way, DB load increases as session activity increases.

Average active executions

The *average active executions (AAE)* per second is related to AAS. To calculate the AAE, Performance Insights divides the total execution time of a query by the time interval. The following table shows the AAE calculation for the same query in the preceding table.

Elapsed time (sec)	Total execution time (sec)	AAE	Calculation
60	120	2	120 execution seconds/60 elapsed seconds
120	120	1	120 execution seconds/120 elapsed seconds

Elapsed time (sec)	Total execution time (sec)	AAE	Calculation
180	380	2.11	380 execution seconds/180 elapsed seconds
240	380	1.58	380 execution seconds/240 elapsed seconds
300	600	2	600 execution seconds/300 elapsed seconds

In most cases, the AAS and AAE for a query are approximately the same. However, because the inputs to the calculations are different data sources, the calculations often vary slightly.

Dimensions

The db.load metric is different from the other time-series metrics because you can break it into subcomponents called *dimensions*. You can think of dimensions as "slice by" categories for the different characteristics of the DBLoad metric.

When you are diagnosing performance issues, the following dimensions are often the most useful:

Topics

- [Wait events \(p. 545\)](#)
- [Top SQL \(p. 546\)](#)
- [Plans \(p. 546\)](#)

For a complete list of dimensions for the Amazon RDS engines, see [DB load sliced by dimensions \(p. 564\)](#).

Wait events

A *wait event* causes a SQL statement to wait for a specific event to happen before it can continue running. Wait events are an important dimension, or category, for DB load because they indicate where work is impeded.

Every active session is either running on the CPU or waiting. For example, sessions consume CPU when they search memory for a buffer, perform a calculation, or run procedural code. When sessions aren't consuming CPU, they might be waiting for a memory buffer to become free, a data file to be read, or a log to be written to. The more time that a session waits for resources, the less time it runs on the CPU.

When you tune a database, you often try to find out the resources that sessions are waiting for. For example, two or three wait events might account for 90 percent of DB load. This measure means that, on average, active sessions are spending most of their time waiting for a small number of resources. If you can find out the cause of these waits, you can attempt a solution.

Consider the analogy of a warehouse worker. An order comes in for a book. The worker might be delayed in fulfilling the order. For example, a different worker might be currently restocking the shelves, a trolley might not be available. Or the system used to enter the order status might be slow. The longer the worker waits, the longer it takes to fulfill the order. Waiting is a natural part of the warehouse workflow, but if wait time becomes excessive, productivity decreases. In the same way, repeated or lengthy session

waits can degrade database performance. For more information, see [Tuning with wait events for Aurora PostgreSQL](#) and [Tuning with wait events for Aurora MySQL](#) in the *Amazon Aurora User Guide*.

Wait events vary by DB engine:

- For information about all MariaDB and MySQL wait events, see [Wait Event Summary Tables](#) in the MySQL documentation.
- For information about all PostgreSQL wait events, see [The Statistics Collector > Wait Event tables](#) in the PostgreSQL documentation.
- For information about all Oracle wait events, see [Descriptions of Wait Events](#) in the Oracle documentation.
- For information about all SQL Server wait events, see [Types of Waits](#) in the SQL Server documentation.

Note

For Oracle, background processes sometimes do work without an associated SQL statement. In these cases, Performance Insights reports the type of background process concatenated with a colon and the wait class associated with that background process. Types of background process include LGWR, ARC0, PMON, and so on.

For example, when the archiver is performing I/O, the Performance Insights report for it is similar to ARC1: System I/O. Occasionally, the background process type is also missing, and Performance Insights only reports the wait class, for example :System I/O.

Top SQL

Where wait events show bottlenecks, top SQL shows which queries are contributing the most to DB load. For example, many queries might be currently running on the database, but a single query might consume 99 percent of the DB load. In this case, the high load might indicate a problem with the query.

By default, the Performance Insights console displays top SQL queries that are contributing to the database load. The console also shows relevant statistics for each statement. To diagnose performance problems for a specific statement, you can examine its execution plan.

Plans

An *execution plan*, also called simply a *plan*, is a sequence of steps that access data. For example, a plan for joining tables t1 and t2 might loop through all rows in t1 and compare each row to a row in t2. In a relational database, an *optimizer* is built-in code that determines the most efficient plan for a SQL query.

For Oracle DB instances, Performance Insights collects execution plans automatically. To diagnose SQL performance problems, examine the captured plans for high-resource Oracle SQL queries. The plans show how Oracle Database has parsed and run queries.

To learn how to analyze DB load using plans, see [Analyzing Oracle execution plans using the Performance Insights dashboard \(p. 581\)](#).

Plan capture

Every five minutes, Performance Insights identifies the most resource-intensive Oracle queries and captures their plans. Thus, you don't need to manually collect and manage a huge number of plans. Instead, you can use the **Top SQL** tab to focus on the plans for the most problematic queries.

Note

Performance Insights doesn't capture plans for queries whose text exceeds the maximum collectable query text limit. For more information, see [Accessing more SQL text in the Performance Insights dashboard \(p. 576\)](#).

The retention period for execution plans is the same as for your Performance Insights data. The retention setting in the free tier is **Default (7 days)**. To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see [Pricing and data retention for Performance Insights \(p. 548\)](#).

Digest queries

The **Top SQL** tab shows digest queries by default. A digest query doesn't itself have a plan, but all queries that use literal values have plans. For example, a digest query might include the text WHERE `email`=? . The digest might contain two queries, one with the text WHERE email=user1@example.com and another with WHERE email=user2@example.com . Each of these literal queries might include multiple plans.

If you select a digest query, the console shows all plans for child statements of the selected digest. Thus, you don't need to look through all the child statements to find the plan. You might see plans that aren't in the displayed list of top 10 child statements. The console shows plans for all child queries for which plans have been collected, regardless of whether the queries are in the top 10.

Maximum CPU

In the dashboard, the **Database load** chart collects, aggregates, and displays session information. To see whether active sessions are exceeding the maximum CPU, look at their relationship to the **Max vCPU** line. The **Max vCPU** value is determined by the number of vCPU (virtual CPU) cores for your DB instance.

One process can run on a vCPU at a time. If the number of processes exceed the number of vCPUs, the processes start queuing. When the queuing increase, the performance is impacted. If the DB load is often above the **Max vCPU** line, and the primary wait state is CPU, the CPU is overloaded. In this case, you might want to throttle connections to the instance, tune any SQL queries with a high CPU load, or consider a larger instance class. High and consistent instances of any wait state indicate that there might be bottlenecks or resource contention issues to resolve. This can be true even if the DB load doesn't cross the **Max vCPU** line.

Amazon RDS DB engine, Region, and instance class support for Performance Insights

Following, you can find the Amazon RDS DB engines that support Performance Insights.

Note

For Amazon Aurora, see [Amazon Aurora DB engine support for Performance Insights in Amazon Aurora User Guide](#).

Amazon RDS DB engine	Supported engine versions and Regions	Instance class restrictions
Amazon RDS for MariaDB	For more information on version and Region availability of Performance Insights with RDS for MariaDB, see Performance Insights (p. 110) .	Performance Insights isn't supported for the following instance classes: <ul style="list-style-type: none">• db.t2.micro• db.t2.small• db.t3.micro• db.t3.small The db.t4g.micro and db.t4g.small instance classes require 10.6 and higher.

Amazon RDS DB engine	Supported engine versions and Regions	Instance class restrictions
RDS for MySQL	For more information on version and Region availability of Performance Insights with RDS for MySQL, see Performance Insights (p. 110) .	Performance Insights isn't supported for the following instance classes: <ul style="list-style-type: none"> • db.t2.micro • db.t2.small • db.t3.micro • db.t3.small The db.t4g instance classes require 8.0.25 and higher version 8.
Amazon RDS for Microsoft SQL Server	For more information on version and Region availability of Performance Insights with RDS for SQL Server, see Performance Insights (p. 110) .	N/A
Amazon RDS for PostgreSQL	For more information on version and Region availability of Performance Insights with RDS for PostgreSQL, see Performance Insights (p. 110) .	N/A
Amazon RDS for Oracle	For more information on version and Region availability of Performance Insights with RDS for Oracle, see Performance Insights (p. 110) .	N/A

Pricing and data retention for Performance Insights

By default, Performance Insights offers a free tier that includes 7 days of performance data history and 1 million API requests per month. You can also purchase longer retention periods. For complete pricing information, see [Performance Insights Pricing](#).

In the RDS console, you can choose any of the following retention periods for your Performance Insights data:

- **Default (7 days)**
- ***n* months**, where *n* is a number from 1–24

Performance Insights [Info](#)

Turn on Performance Insights [Info](#)

Retention period [Info](#)

7 days (free tier)	▲
7 days (free tier)	
1 month	
2 months	
3 months	
4 months	
5 months	
6 months	
7 months	
8 months	
9 months	
10 months	
11 months	
12 months	
13 months	
14 months	

To learn how to set a retention period using the AWS CLI, see [AWS CLI \(p. 551\)](#).

Turning Performance Insights on and off

You can turn on Performance Insights for your DB instance or Multi-AZ DB cluster when you create it. If needed, you can turn it off later. Turning Performance Insights on and off doesn't cause downtime, a reboot, or a failover.

Note

Performance Schema is an optional performance tool used by Amazon RDS for MariaDB or MySQL. If you turn Performance Schema on or off, you need to reboot. If you turn Performance Insights on or off, however, you don't need to reboot. For more information, see [Turning on the Performance Schema for Performance Insights on Amazon RDS for MariaDB or MySQL \(p. 553\)](#).

The Performance Insights agent consumes limited CPU and memory on the DB host. When the DB load is high, the agent limits the performance impact by collecting data less frequently.

Console

In the console, you can turn Performance Insights on or off when you create or modify a DB instance or Multi-AZ DB cluster.

Turning Performance Insights on or off when creating a DB instance or Multi-AZ DB cluster

When you create a new DB instance or Multi-AZ DB cluster, turn on Performance Insights by choosing **Enable Performance Insights** in the **Performance Insights** section. Or choose **Disable Performance Insights**. For more information, see the following topics:

- To create a DB instance, follow the instructions for your DB engine in [Creating an Amazon RDS DB instance \(p. 230\)](#).
- To create a Multi-AZ DB cluster, follow the instructions for your DB engine in [Creating a Multi-AZ DB cluster \(p. 252\)](#).

The following screenshot shows the **Performance Insights** section.



If you choose **Enable Performance Insights**, you have the following options:

- **Retention** – The amount of time to retain Performance Insights data. The retention setting in the free tier is **Default (7 days)**. To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see [Pricing and data retention for Performance Insights \(p. 548\)](#).
- **AWS KMS key** – Specify your AWS KMS key. Performance Insights encrypts all potentially sensitive data using your KMS key. Data is encrypted in flight and at rest. For more information, see [Configuring an AWS KMS policy for Performance Insights \(p. 558\)](#).

Turning Performance Insights on or off when modifying a DB instance or Multi-AZ DB cluster

In the console, you can modify a DB instance or Multi-AZ DB cluster to turn Performance Insights on or off.

To turn Performance Insights on or off for a DB instance or Multi-AZ DB cluster using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Databases**.
3. Choose a DB instance or Multi-AZ DB cluster, and choose **Modify**.
4. In the **Performance Insights** section, choose either **Enable Performance Insights** or **Disable Performance Insights**.

If you choose **Enable Performance Insights**, you have the following options:

- **Retention** – The amount of time to retain Performance Insights data. The retention setting in the free tier is **Default (7 days)**. To retain your performance data for longer, specify 1–24 months. For more information about retention periods, see [Pricing and data retention for Performance Insights \(p. 548\)](#).
 - **AWS KMS key** – Specify your KMS key. Performance Insights encrypts all potentially sensitive data using your KMS key. Data is encrypted in flight and at rest. For more information, see [Encrypting Amazon RDS resources \(p. 2000\)](#).
5. Choose **Continue**.
 6. For **Scheduling of Modifications**, choose **Apply immediately**. If you choose **Apply during the next scheduled maintenance window**, your instance ignores this setting and turns on Performance Insights immediately.
 7. Choose **Modify instance**.

AWS CLI

When you use the [create-db-instance](#) AWS CLI command, turn on Performance Insights by specifying `--enable-performance-insights`. Or turn off Performance Insights by specifying `--no-enable-performance-insights`.

You can also specify these values using the following AWS CLI commands:

- [create-db-instance-read-replica](#)
- [modify-db-instance](#)
- [restore-db-instance-from-s3](#)
- [create-db-cluster](#) (Multi-AZ DB cluster)
- [modify-db-cluster](#) (Multi-AZ DB cluster)

The following procedure describes how to turn Performance Insights on or off for an existing DB instance using the AWS CLI.

To turn Performance Insights on or off for a DB instance using the AWS CLI

- Call the [modify-db-instance](#) AWS CLI command and supply the following values:
 - `--db-instance-identifier` – The name of the DB instance.
 - `--enable-performance-insights` to turn on or `--no-enable-performance-insights` to turn off

The following example turns on Performance Insights for `sample-db-instance`.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier sample-db-instance \
  --enable-performance-insights
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier sample-db-instance ^
```

```
--enable-performance-insights
```

When you turn on Performance Insights in the CLI, you can optionally specify the number of days to retain Performance Insights data with the `--performance-insights-retention-period` option. You can specify 7, *month* * 31 (where *month* is a number from 1–23), or 731. For example, if you want to retain your performance data for 3 months, specify 93, which is 3 * 31. The default is 7 days. For more information about retention periods, see [Pricing and data retention for Performance Insights \(p. 548\)](#).

The following example turns on Performance Insights for `sample-db-instance` and specifies that Performance Insights data is retained for 93 days (3 months).

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier sample-db-instance \
  --enable-performance-insights \
  --performance-insights-retention-period 93
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier sample-db-instance ^
  --enable-performance-insights ^
  --performance-insights-retention-period 93
```

If you specify a retention period such as 94 days, which isn't a valid value, RDS issues an error.

```
An error occurred (InvalidParameterValue) when calling the CreateDBInstance operation:
Invalid Performance Insights retention period. Valid values are: [7, 31, 62, 93, 124, 155,
186, 217,
248, 279, 310, 341, 372, 403, 434, 465, 496, 527, 558, 589, 620, 651, 682, 713, 731]
```

RDS API

When you create a new DB instance using the [CreateDBInstance](#) operation Amazon RDS API operation, turn on Performance Insights by setting `EnablePerformanceInsights` to `True`. To turn off Performance Insights, set `EnablePerformanceInsights` to `False`.

You can also specify the `EnablePerformanceInsights` value using the following API operations:

- [ModifyDBInstance](#)
- [CreateDBInstanceReadReplica](#)
- [RestoreDBInstanceFromS3](#)
- [CreateDBCluster](#) (Multi-AZ DB cluster)
- [ModifyDBCluster](#) (Multi-AZ DB cluster)

When you turn on Performance Insights, you can optionally specify the amount of time, in days, to retain Performance Insights data with the `PerformanceInsightsRetentionPeriod` parameter. You can specify 7, *month* * 31 (where *month* is a number from 1–23), or 731. For example, if you want to retain your performance data for 3 months, specify 93, which is 3 * 31. The default is 7 days. For more information about retention periods, see [Pricing and data retention for Performance Insights \(p. 548\)](#).

Turning on the Performance Schema for Performance Insights on Amazon RDS for MariaDB or MySQL

The Performance Schema is an optional feature for monitoring Amazon RDS for MariaDB or MySQL runtime performance at a low level of detail. The Performance Schema is designed to have minimal impact on database performance. Performance Insights is a separate feature that you can use with or without the Performance Schema.

Topics

- [Overview of the Performance Schema \(p. 553\)](#)
- [Performance Insights and the Performance Schema \(p. 553\)](#)
- [Automatic management of the Performance Schema by Performance Insights \(p. 554\)](#)
- [Effect of a reboot on the Performance Schema \(p. 554\)](#)
- [Determining whether Performance Insights is managing the Performance Schema \(p. 555\)](#)
- [Configuring the Performance Schema for automatic management \(p. 555\)](#)

Overview of the Performance Schema

The Performance Schema monitors events in MariaDB and MySQL databases. An *event* is a database server action that consumes time and has been instrumented so that timing information can be collected. Examples of events include the following:

- Function calls
- Waits for the operating system
- Stages of SQL execution
- Groups of SQL statements

The PERFORMANCE_SCHEMA storage engine is a mechanism for implementing the Performance Schema feature. This engine collects event data using instrumentation in the database source code. The engine stores events in memory-only tables in the performance_schema database. You can query performance_schema just as you can query any other tables. For more information, see [MySQL Performance Schema](#) in the *MySQL Reference Manual*.

Performance Insights and the Performance Schema

Performance Insights and the Performance Schema are separate features, but they are connected. The behavior of Performance Insights for Amazon RDS for MariaDB or MySQL depends on whether the Performance Schema is turned on, and if so, whether Performance Insights manages the Performance Schema automatically. The following table describes the behavior.

Performance Schema turned on	Performance Insights management mode	Performance Insights behavior
Yes	Automatic	<ul style="list-style-type: none">• Collects detailed, low-level monitoring information• Collects active session metrics every second• Displays DB load categorized by detailed wait events, which you can use to identify bottlenecks
Yes	Manual	<ul style="list-style-type: none">• Collects wait events and per-SQL metrics

Performance Schema turned on	Performance Insights management mode	Performance Insights behavior
		<ul style="list-style-type: none"> Collects active session metrics every five seconds instead of every second Reports user states such as inserting and sending, which don't help you identify bottlenecks
No	N/A	<ul style="list-style-type: none"> Doesn't collect wait events, per-SQL metrics, or other detailed, low-level monitoring information Collects active session metrics every five seconds instead of every second Reports user states such as inserting and sending, which don't help you identify bottlenecks

Automatic management of the Performance Schema by Performance Insights

When you create an Amazon RDS for MariaDB or MySQL DB instance with Performance Insights turned on, the Performance Schema is also turned on. In this case, Performance Insights automatically manages your Performance Schema parameters. This is the recommended configuration.

Note

Automatic management of the Performance Schema isn't supported for the t4g.medium instance class.

For automatic management of the Performance Schema, the following conditions must be true:

- The `performance_schema` parameter is set to `0`.
- The **Source** is set to `system`, which is the default.

If you change the `performance_schema` parameter value manually, and then later want to change to automatic management, see [Configuring the Performance Schema for automatic management \(p. 555\)](#).

Important

When Performance Insights turns on the Performance Schema, it doesn't change the parameter group values. However, the values are changed on the DB instances that are running. The only way to see the changed values is to run the `SHOW GLOBAL VARIABLES` command.

Effect of a reboot on the Performance Schema

Performance Insights and the Performance Schema differ in their requirements for DB instance reboots:

Performance Schema

To turn this feature on or off, you must reboot the DB instance.

Performance Insights

To turn this feature on or off, you don't need to reboot the DB instance.

If the Performance Schema isn't currently turned on, and you turn on Performance Insights without rebooting the DB instance, the Performance Schema won't be turned on.

Determining whether Performance Insights is managing the Performance Schema

To find out whether Performance Insights is currently managing the Performance Schema for major engine versions 5.6, 5.7, and 8.0, review the following table.

Setting of performance_schema parameter	Setting of the Source column	Performance Insights is managing the Performance Schema?
0	system	Yes
0 or 1	user	No

To determine whether Performance Insights is managing the Performance Schema automatically

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Parameter groups**.
3. Select the name of the parameter group for your DB instance.
4. Enter **performance_schema** in the search bar.
5. Check whether **Source** is the system default and **Values** is **0**. If so, Performance Insights is managing the Performance Schema automatically. If not, Performance Insights isn't managing the Performance Schema automatically.

The screenshot shows the 'Parameters' section of the AWS RDS Parameter Groups configuration. A search bar at the top contains 'performance_schema'. Below it, a table lists parameters. The 'performance_schema' parameter is selected, showing its current value as '0' in the 'Values' dropdown, which is highlighted with a red box. The 'Source' dropdown also has a red box around its value 'user'.

Name	Values	Allowed values	Modifiable	Source
performance_schema	0	0, 1	true	user

Configuring the Performance Schema for automatic management

Assume that Performance Insights is turned on for your DB instance or Multi-AZ DB cluster but isn't currently managing the Performance Schema. If you want to allow Performance Insights to manage the Performance Schema automatically, complete the following steps.

To configure the Performance Schema for automatic management

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Parameter groups**.
3. Select the name of the parameter group for your DB instance or Multi-AZ DB cluster.
4. Enter **performance_schema** in the search bar.
5. Select the **performance_schema** parameter.
6. Choose **Edit parameters**.
7. Select the **performance_schema** parameter.

8. In **Values**, choose **0**.
9. Choose **Reset** and then **Reset parameters**.
10. Reboot the DB instance or Multi-AZ DB cluster.

Important

Whenever you turn the Performance Schema on or off, make sure to reboot the DB instance or Multi-AZ DB cluster.

For more information about modifying instance parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#). For more information about the dashboard, see [Analyzing metrics with the Performance Insights dashboard \(p. 559\)](#). For more information about the MySQL performance schema, see [MySQL 8.0 Reference Manual](#).

Configuring access policies for Performance Insights

To access Performance Insights, a principal must have the appropriate permissions from AWS Identity and Access Management (IAM). You can grant access in the following ways:

- Attach the `AmazonRDSPerformanceInsightsReadOnly` managed policy to an IAM user or role.
- Create a custom IAM policy and attach it to an IAM user or role.

If you specified a customer managed key when you turned on Performance Insights, make sure that users in your account have the `kms:Decrypt` and `kms:GenerateDataKey` permissions on the KMS key.

Attaching the `AmazonRDSPerformanceInsightsReadOnly` policy to an IAM principal

`AmazonRDSPerformanceInsightsReadOnly` is an AWS-managed policy that grants access to all read-only operations of the Amazon RDS Performance Insights API. Currently, all operations in this API are read-only.

If you attach `AmazonRDSPerformanceInsightsReadOnly` to an IAM user or role, the recipient can use Performance Insights with other console features.

Creating a custom IAM policy for Performance Insights

For users who don't have the `AmazonRDSPerformanceInsightsReadOnly` policy, you can grant access to Performance Insights by creating or modifying a user-managed IAM policy. When you attach the policy to an IAM user or role, the recipient can use Performance Insights.

To create a custom policy

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose **Policies**.
3. Choose **Create policy**.
4. On the **Create Policy** page, choose the **JSON** tab.
5. Copy and paste the following text, replacing `us-east-1` with the name of your AWS Region and `111122223333` with your customer account number.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "rds:DescribePerformanceInsights",  
            "Resource": "arn:aws:rds:us-east-1:111122223333:*:performance-insights/*"  
        }  
    ]  
}
```

```

        "Action": "rds:DescribeDBInstances",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "rds:DescribeDBClusters",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "pi:DescribeDimensionKeys",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    },
    {
        "Effect": "Allow",
        "Action": "pi:GetDimensionKeyDetails",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    },
    {
        "Effect": "Allow",
        "Action": "pi:GetResourceMetadata",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    },
    {
        "Effect": "Allow",
        "Action": "pi:GetResourceMetrics",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    },
    {
        "Effect": "Allow",
        "Action": "pi>ListAvailableResourceDimensions",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    },
    {
        "Effect": "Allow",
        "Action": "pi>ListAvailableResourceMetrics",
        "Resource": "arn:aws:pi:us-east-1:111122223333:metrics/rds/*"
    }
]
}

```

6. Choose **Review policy**.
7. Provide a name for the policy and optionally a description, and then choose **Create policy**.

You can now attach the policy to an IAM user or role. The following procedure assumes that you already have an IAM user available for this purpose.

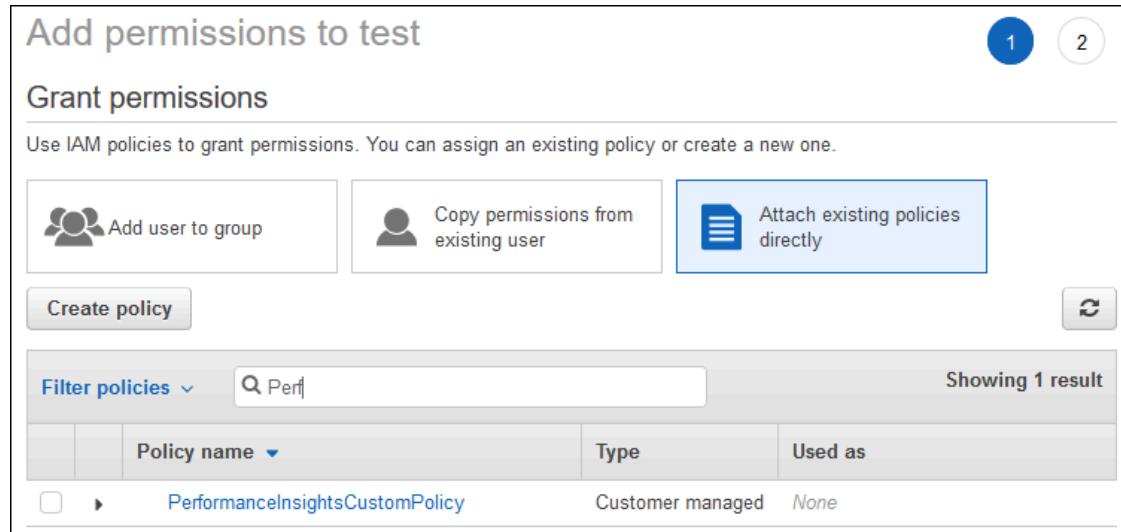
To attach the policy to an IAM user

1. Open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane, choose **Users**.
3. Choose an existing user from the list.

Important

To use Performance Insights, make sure that you have access to Amazon RDS in addition to the custom policy. For example, the `AmazonRDSPerformanceInsightsReadOnly` predefined policy provides read-only access to Amazon RDS. For more information, see [Managing access using policies \(p. 2018\)](#).

4. On the **Summary** page, choose **Add permissions**.
5. Choose **Attach existing policies directly**. For **Search**, type the first few characters of your policy name, as shown following.



6. Choose your policy, and then choose **Next: Review**.
7. Choose **Add permissions**.

Configuring an AWS KMS policy for Performance Insights

Performance Insights uses an AWS KMS key to encrypt sensitive data. When you enable Performance Insights through the API or the console, you can do either of the following:

- Choose the default AWS managed key.

Amazon RDS uses the AWS managed key for your new DB instance. Amazon RDS creates an AWS managed key for your AWS account. Your AWS account has a different AWS managed key for Amazon RDS for each AWS Region.

- Choose a customer managed key.

If you specify a customer managed key, users in your account that call the Performance Insights API need the `kms:Decrypt` and `kms:GenerateDataKey` permissions on the KMS key. You can configure these permissions through IAM policies. However, we recommend that you manage these permissions through your KMS key policy. For more information, see [Using key policies in AWS KMS](#).

Example

The following example shows how to add statements to your KMS key policy. These statements allow access to Performance Insights. Depending on how you use the KMS key, you might want to change some restrictions. Before adding statements to your policy, remove all comments.

```
{
  "Version" : "2012-10-17",
  "Id" : "your-policy",
  "Statement" : [ {
    //This represents a statement that currently exists in your policy.
  }
  ....,
  //Starting here, add new statement to your policy for Performance Insights.
  //We recommend that you add one new statement for every RDS instance
{
    "Sid" : "Allow viewing RDS Performance Insights",
    "Effect": "Allow",
  }
}
```

```
"Principal": {  
    "AWS": [  
        //One or more principals allowed to access Performance Insights  
        "arn:aws:iam::444455556666:role/Role1"  
    ]  
},  
"Action": [  
    "kms:Decrypt",  
    "kms:GenerateDataKey"  
],  
"Resource": "*",  
"Condition" : {  
    "StringEquals" : {  
        //Restrict access to only RDS APIs (including Performance Insights).  
        //Replace region with your AWS Region.  
        //For example, specify us-west-2.  
        "kms:ViaService" : "rds.region.amazonaws.com"  
    },  
    "ForAnyValue:StringEquals": {  
        //Restrict access to only data encrypted by Performance Insights.  
        "kms:EncryptionContext:aws:pi:service": "rds",  
        "kms:EncryptionContext:service": "pi",  
  
        //Restrict access to a specific RDS instance.  
        //The value is a DbiResourceId.  
        "kms:EncryptionContext:aws:rds:db-id": "db-AAAAABBBBBCCCCDDDDDEEEEEE"  
    }  
}  
}
```

Analyzing metrics with the Performance Insights dashboard

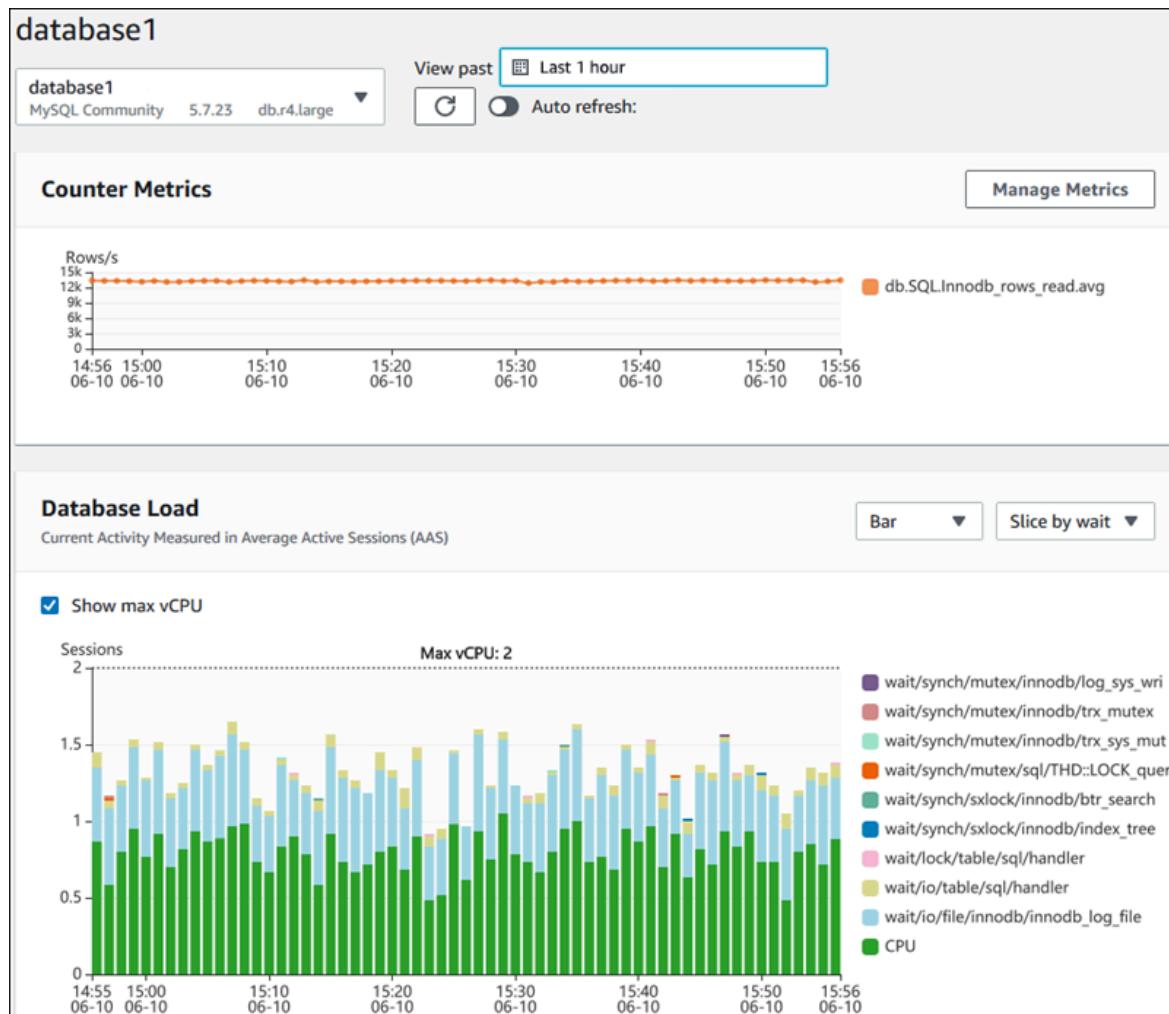
The Performance Insights dashboard contains database performance information to help you analyze and troubleshoot performance issues. On the main dashboard page, you can view information about the database load. You can "slice" DB load by dimensions such as wait events or SQL.

Performance Insights dashboard

- [Overview of the Performance Insights dashboard \(p. 559\)](#)
- [Accessing the Performance Insights dashboard \(p. 567\)](#)
- [Analyzing DB load by wait events \(p. 569\)](#)
- [Analyzing queries in the Performance Insights dashboard \(p. 570\)](#)
- [Analyzing Oracle execution plans using the Performance Insights dashboard \(p. 581\)](#)

Overview of the Performance Insights dashboard

The dashboard is the easiest way to interact with Performance Insights. The following example shows the dashboard for a MySQL DB instance.

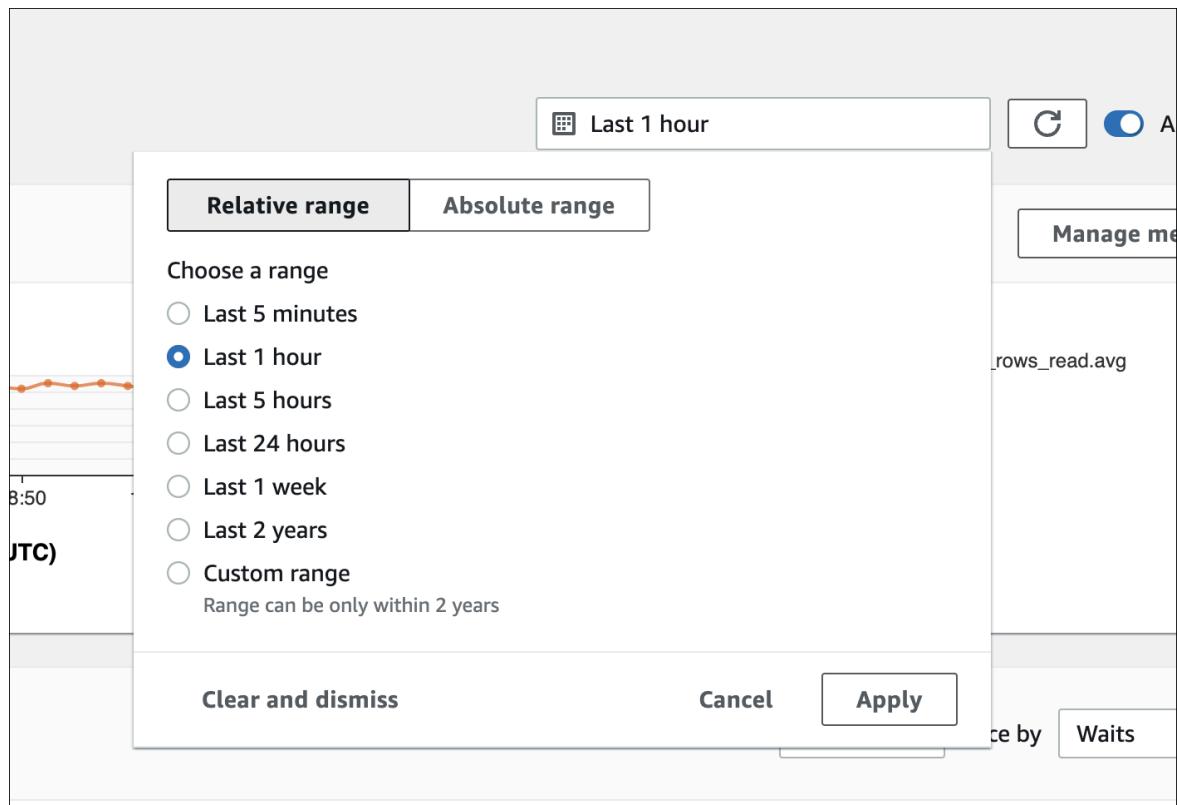


Topics

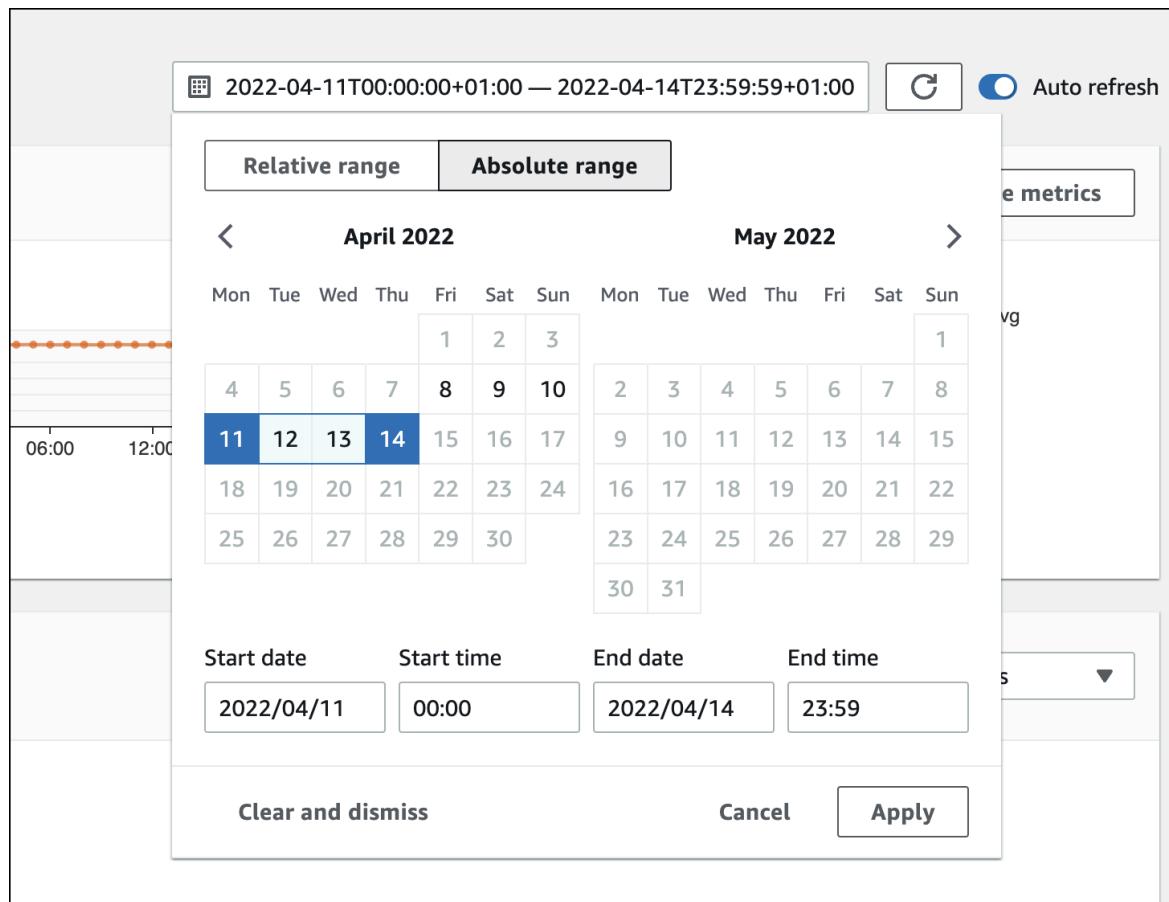
- [Time range filter \(p. 560\)](#)
- [Counter metrics chart \(p. 562\)](#)
- [Database load chart \(p. 564\)](#)
- [Top dimensions table \(p. 566\)](#)

Time range filter

By default, the Performance Insights dashboard shows DB load for the last hour. You can adjust this range to be as short as 5 minutes or as long as 2 years. You can also select a custom relative range.



You can select an absolute range with a beginning and ending date and time. The following example shows the time range beginning at midnight on 4/11/22 and ending at 11:59 PM on 4/14/22.

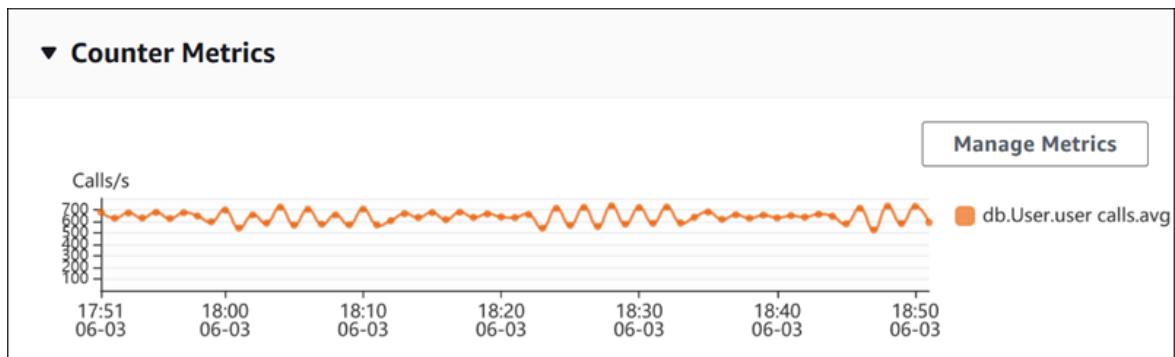


Counter metrics chart

With counter metrics, you can customize the Performance Insights dashboard to include up to 10 additional graphs. These graphs show a selection of dozens of operating system and database performance metrics. You can correlate this information with DB load to help identify and analyze performance problems.

The **Counter metrics** chart displays data for performance counters. The default metrics depend on the DB engine:

- MySQL and MariaDB – db.SQL.Innodb_rows_read.avg
- Oracle – db.User.user_calls.avg
- Microsoft SQL Server – db.Databases.Active_Transactions(_Total).avg
- PostgreSQL – db.Transactions.xact_commit.avg



To change the performance counters, choose **Manage Metrics**. You can select multiple **OS metrics** or **Database metrics**, as shown in the following screenshot. To see details for any metric, hover over the metric name.

This screenshot shows the 'Select metrics shown on the graph' dialog. It includes a search bar, tabs for 'OS metrics' (0) and 'Database metrics' (1), and a 'Clear all selections' button. The 'Database metrics' tab is selected. The interface is organized into sections: 'User' (with 'user calls' checked), 'Redo' (empty), 'Cache' (empty), and 'SQL' (empty). At the bottom are 'Cancel' and 'Update graph' buttons.

Select metrics shown on the graph

Check the metrics that you want to see on the Performance Insights dashboard.

Find metrics

OS metrics (0) Database metrics (1) Clear all selections

CPU used by this session SQL*Net roundtrips to/from client bytes received via SQL*Net from client
 user commits logons cumulative user calls
 bytes sent via SQL*Net to client user rollbacks

redo size

Cache

physical read bytes db block gets DBWR checkpoints
 physical reads consistent gets from cache db block gets from cache
 consistent gets

SQL

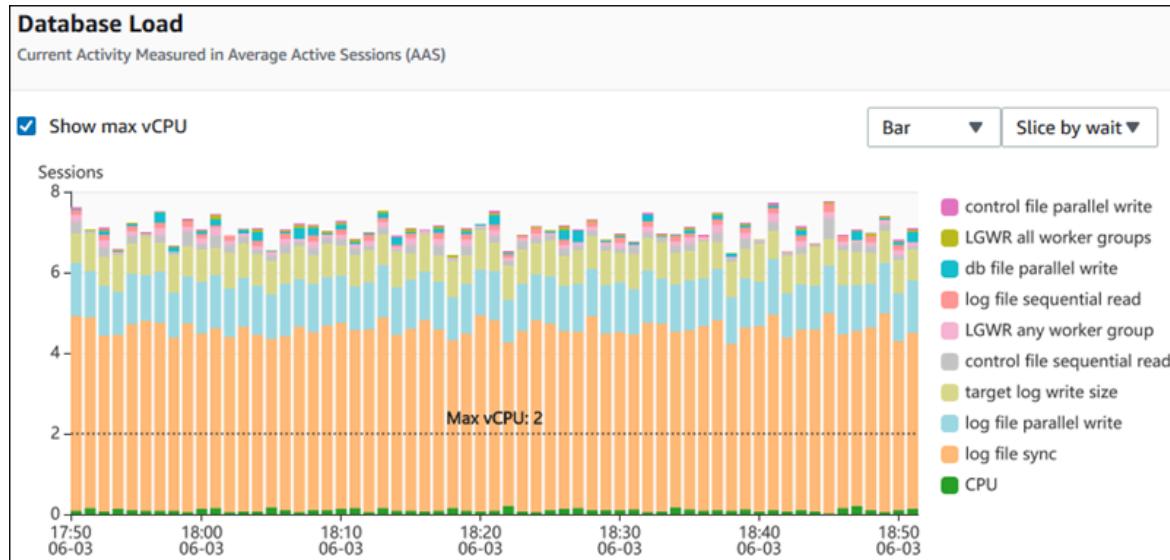
parse count (total) parse count (hard) table scan rows gotten
 sorts (memory) sorts (disk) sorts (rows)

Cancel Update graph

For descriptions of the counter metrics that you can add for each DB engine, see [Performance Insights counter metrics \(p. 618\)](#).

Database load chart

The **Database load** chart shows how the database activity compares to DB instance capacity as represented by the **Max vCPU** line. By default, the stacked line chart represents DB load as average active sessions per unit of time. The DB load is sliced (grouped) by wait states.

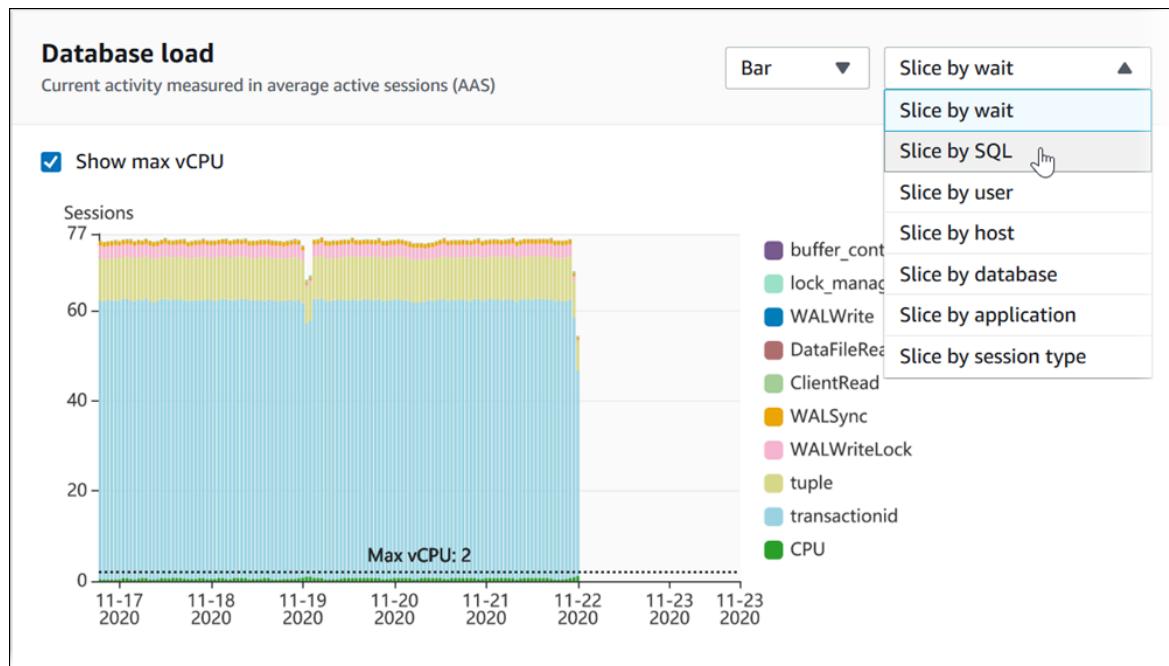


DB load sliced by dimensions

You can choose to display load as active sessions grouped by any supported dimensions. The following table shows which dimensions are supported for the different engines.

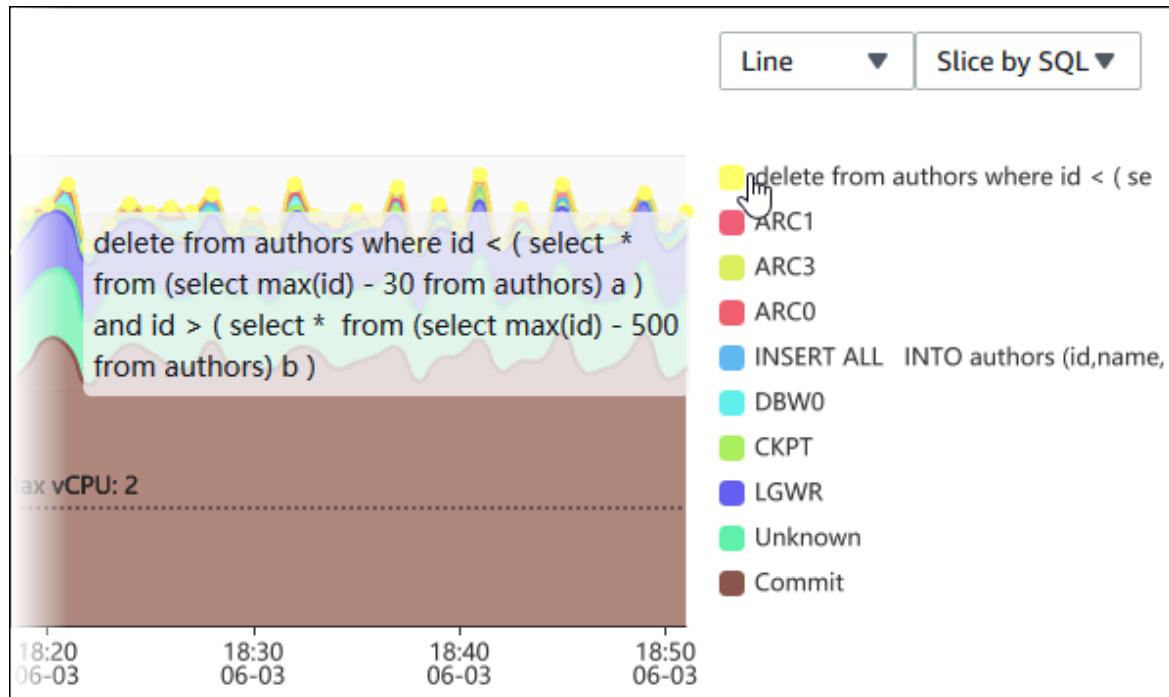
Dimension	Oracle	SQL Server	PostgreSQL	MySQL
Host	Yes	Yes	Yes	Yes
SQL	Yes	Yes	Yes	Yes
User	Yes	Yes	Yes	Yes
Waits	Yes	Yes	Yes	Yes
Plans	Yes	No	No	No
Application	No	No	Yes	No
Database	No	No	Yes	Yes
Session type	No	No	Yes	No

The following image shows the dimensions for a PostgreSQL DB instance.

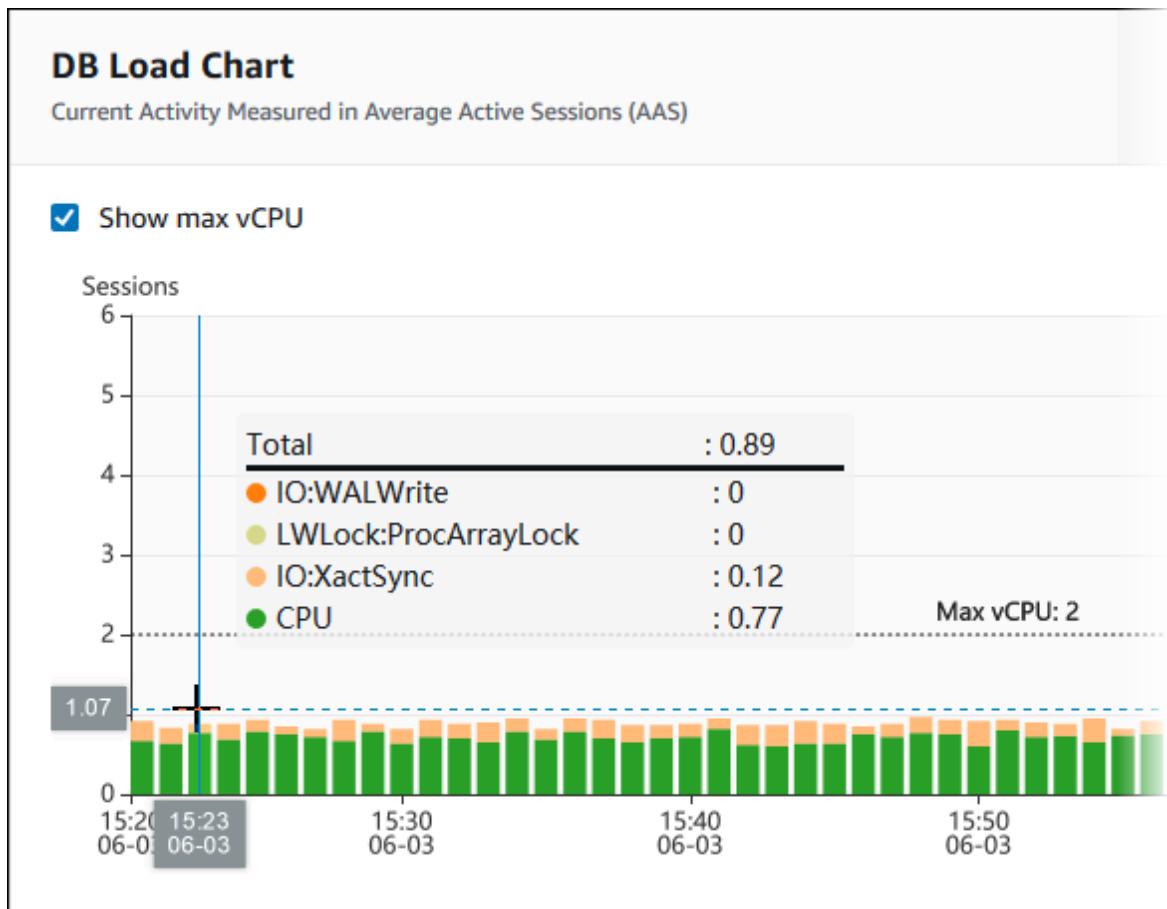


DB load details for a dimension item

To see details about a DB load item within a dimension, hover over the item name. The following image shows details for a SQL statement.



To see details for any item for the selected time period in the legend, hover over that item.



Top dimensions table

The Top dimensions table slices DB load by different dimensions. A dimension is a category or "slice by" for different characteristics of DB load. If the dimension is SQL, **Top SQL** shows the SQL statements that contribute the most to DB load.

Top waits	Top SQL	Top hosts	Top users	Top connections	Top databases	Top applications	Top session types
Top SQL (0) Learn more							
<input type="text"/> Find SQL statements							
Load by waits (AAS)				SQL statements			

Choose any of the following dimension tabs.

Tab	Description	Supported engines
Top SQL	The SQL statements that are currently running	All
Top waits	The event for which the database backend is waiting	All

Tab	Description	Supported engines
Top hosts	The host name of the connected client	All
Top users	The user logged in to the database	All
Top databases	The name of the database to which the client is connected	PostgreSQL, MySQL, and MariaDB only
Top applications	The name of the application that is connected to the database	PostgreSQL only
Top session types	The type of the current session	PostgreSQL only

To learn how to analyze queries by using the **Top SQL** tab, see [Overview of the Top SQL tab \(p. 571\)](#).

Accessing the Performance Insights dashboard

To access the Performance Insights dashboard, use the following procedure.

To view the Performance Insights dashboard in the AWS Management Console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the left navigation pane, choose **Performance Insights**.
3. Choose a DB instance.

The Performance Insights dashboard is shown for that DB instance.

For DB instances with Performance Insights turned on, you can also reach the dashboard by choosing the **Sessions** item in the list of DB instances. Under **Current activity**, the **Sessions** item shows the database load in average active sessions over the last five minutes. The bar graphically shows the load. When the bar is empty, the DB instance is idle. As the load increases, the bar fills with blue. When the load passes the number of virtual CPUs (vCPUs) on the DB instance class, the bar turns red, indicating a potential bottleneck.

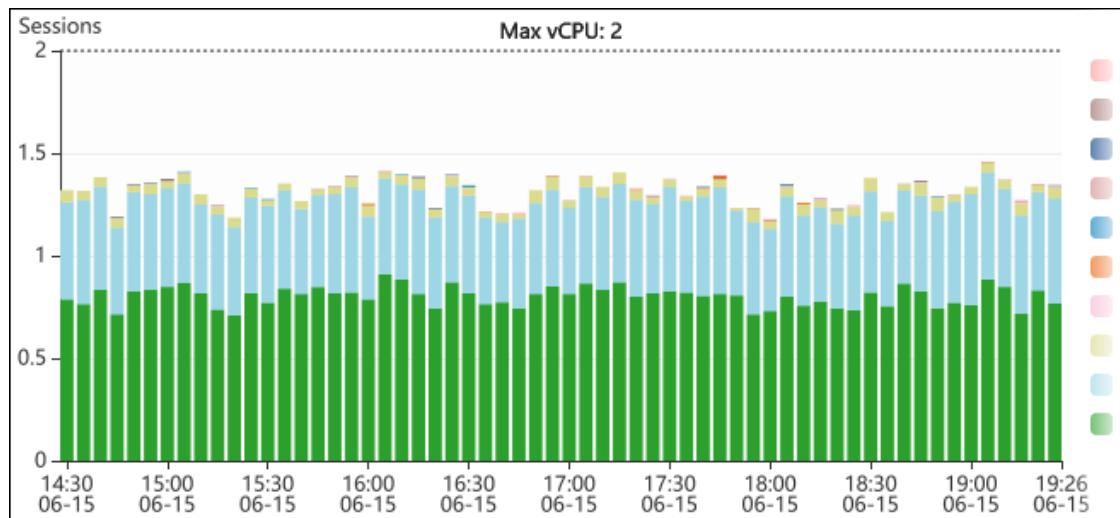
Databases		Group resources	Actions	Restore from S3	Create database
<input type="checkbox"/>	DB identifier	<input checked="" type="radio"/> Filter databases			
<input type="checkbox"/>	database1	MySQL Community	<div style="width: 45.51%;">45.51%</div>	<div style="width: 1.34%;">1.34 Sessions</div>	
<input type="checkbox"/>	database2	Oracle Enterprise Edition	<div style="width: 55.41%;">55.41%</div>	<div style="width: 3.48%;">3.48 Sessions</div>	
<input type="checkbox"/>	database3	Oracle Enterprise Edition	<div style="width: 1.02%;">1.02%</div>	<div style="width: 0%;">0 Connections</div>	

4. (Optional) Choose **View past** in the upper right and specify a different relative or absolute time interval.

In the following example, the DB load is shown for the last 5 hours.

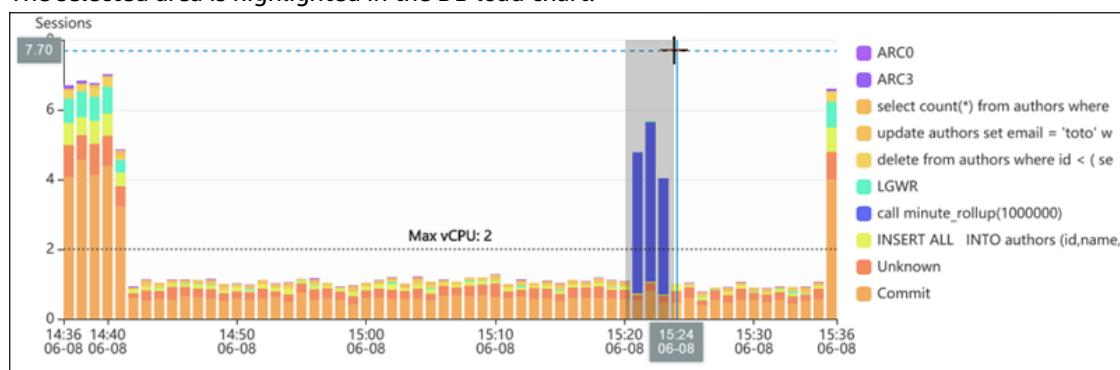


In the following screenshot, the DB load interval is 5 hours.

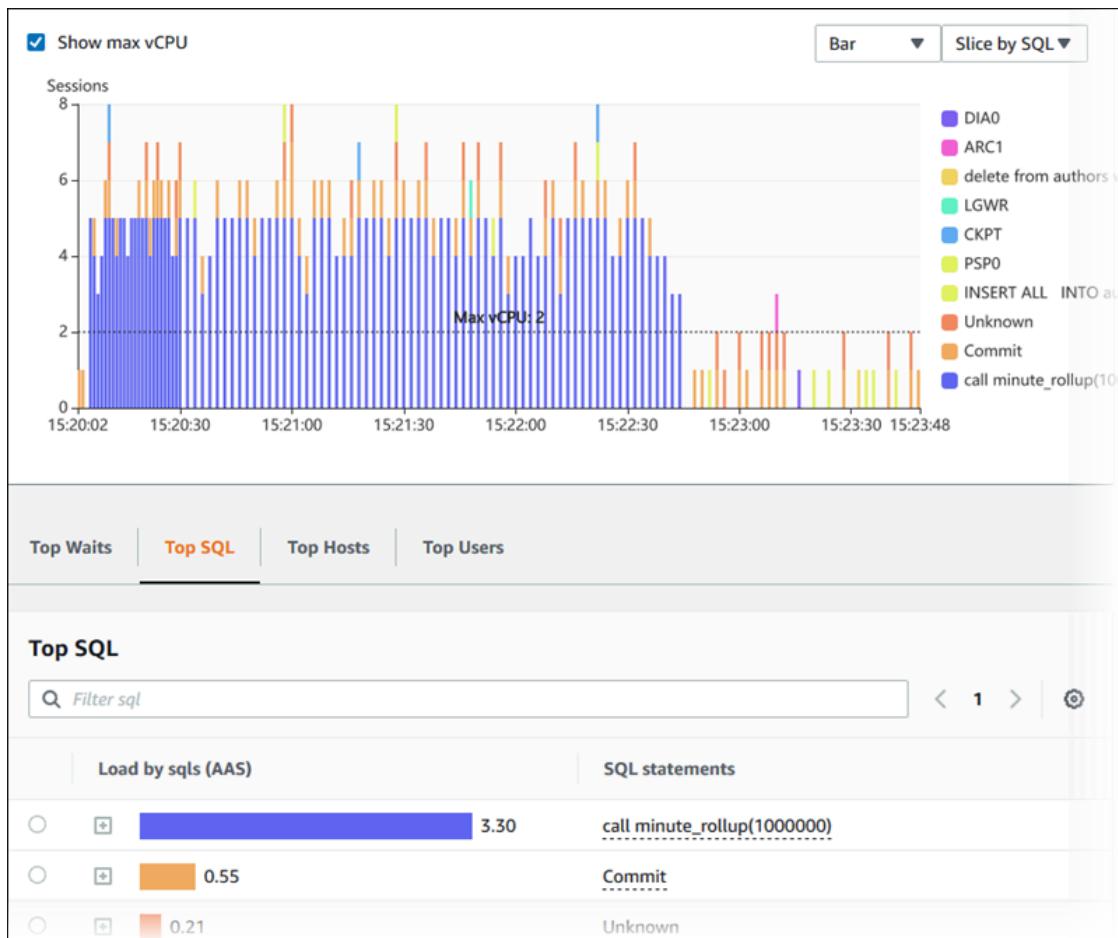


5. (Optional) To zoom in on a portion of the DB load chart, choose the start time and drag to the end of the time period you want.

The selected area is highlighted in the DB load chart.



When you release the mouse, the DB load chart zooms in on the selected AWS Region, and the **Top dimensions** table is recalculated.



6. (Optional) To refresh your data automatically, enable **Auto refresh**.



The Performance Insight dashboard automatically refreshes with new data. The refresh rate depends on the amount of data displayed:

- 5 minutes refreshes every 5 seconds.
- 1 hour refreshes every minute.
- 5 hours refreshes every minute.
- 24 hours refreshes every 5 minutes.
- 1 week refreshes every hour.

Analyzing DB load by wait events

If the **Database load** chart shows a bottleneck, you can find out where the load is coming from. To do so, look at the top load items table below the **Database load** chart. Choose a particular item, like a SQL query or a user, to drill down into that item and see details about it.

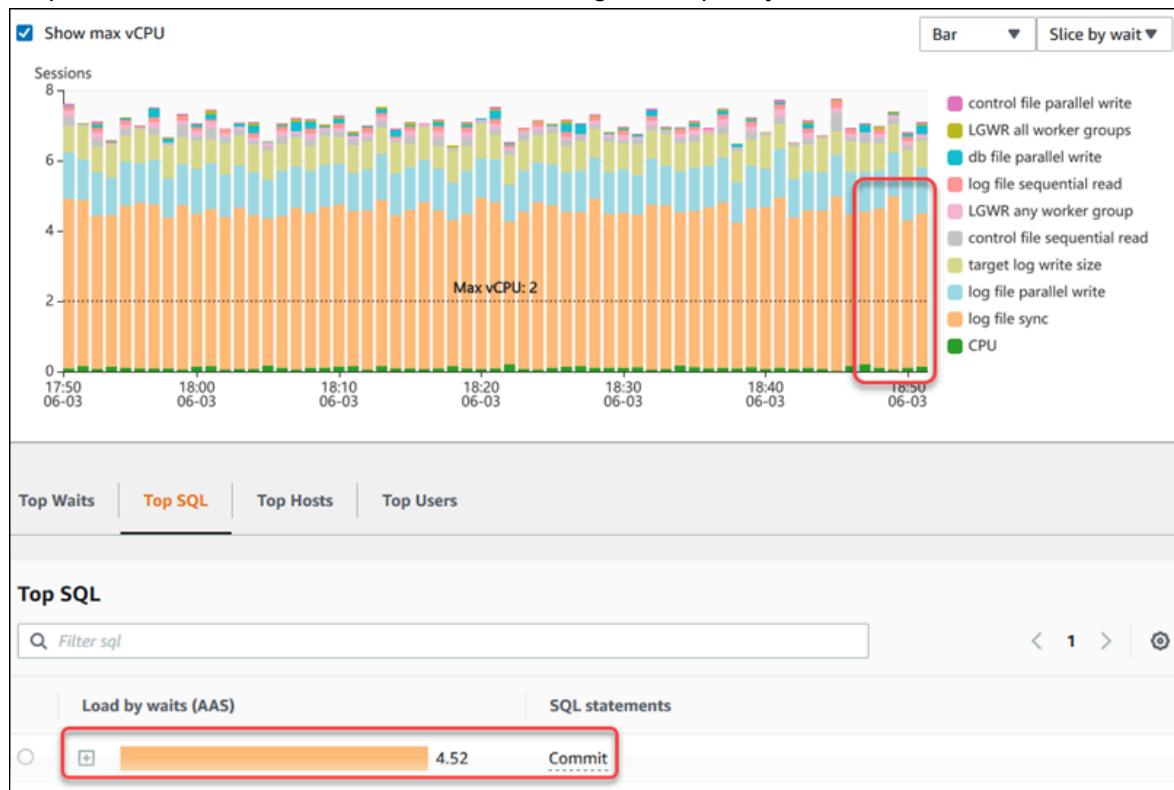
DB load grouped by waits and top SQL queries is the default Performance Insights dashboard view. This combination typically provides the most insight into performance issues. DB load grouped by waits

shows if there are any resource or concurrency bottlenecks in the database. In this case, the **SQL** tab of the top load items table shows which queries are driving that load.

Your typical workflow for diagnosing performance issues is as follows:

1. Review the **Database load** chart and see if there are any incidents of database load exceeding the **Max CPU** line.
2. If there is, look at the **Database load** chart and identify which wait state or states are primarily responsible.
3. Identify the digest queries causing the load by seeing which of the queries the **SQL** tab on the top load items table are contributing most to those wait states. You can identify these by the **DB Load by Wait** column.
4. Choose one of these digest queries in the **SQL** tab to expand it and see the child queries that it is composed of.

For example, in the dashboard following, **log file sync** waits account for most of the DB load. The **LGWR all worker groups** wait is also high. The **Top SQL** chart shows what is causing the **log file sync** waits: frequent COMMIT statements. In this case, committing less frequently will reduce DB load.



Analyzing queries in the Performance Insights dashboard

In the Amazon RDS Performance Insights dashboard, you can find information about running and recent queries in the **Top SQL** tab in the **Top dimensions** table. You can use this information to tune your queries.

Note

RDS for SQL Server doesn't show SQL-level statistics.

Topics

- [Overview of the Top SQL tab \(p. 571\)](#)
- [Accessing more SQL text in the Performance Insights dashboard \(p. 576\)](#)
- [Viewing SQL statistics in the Performance Insights dashboard \(p. 578\)](#)

Overview of the Top SQL tab

By default, the **Top SQL** tab shows the 25 queries that are contributing the most to DB load. To help tune your queries, you can analyze information such as the query text and SQL statistics. You can also choose the statistics that you want to appear in the **Top SQL** tab.

Topics

- [SQL text \(p. 571\)](#)
- [SQL statistics \(p. 572\)](#)
- [Load by waits \(AAS\) \(p. 573\)](#)
- [SQL information \(p. 573\)](#)
- [Preferences \(p. 574\)](#)

SQL text

By default, each row in the **Top SQL** table shows 500 bytes of text for each statement.

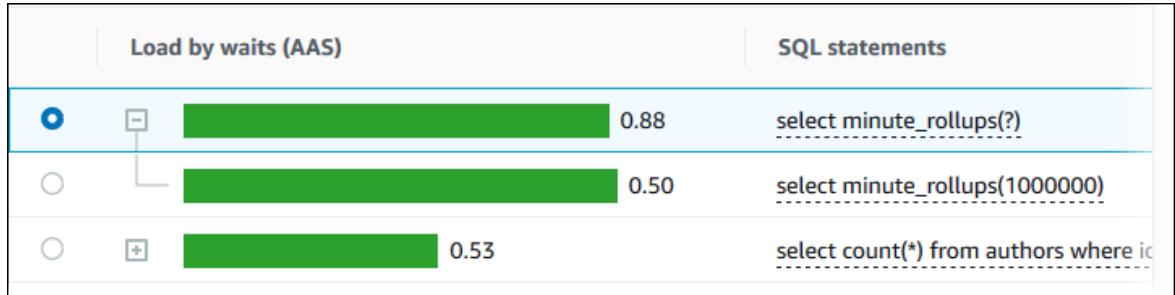
Top SQL (10) Learn more	
<input type="text"/> Find SQL statements	
Load by waits (AAS)	SQL statements
2.00	SELECT SEAT_LEVEL, SEAT_SECTION, SEAT_ROW FROM (SELECT SEAT_LEVEL, SEAT_SECTION, S...
1.71	select p.full_name, SUM(t.id) from ticket_purchase_hist h, person p, sporting_e...
1.17	SELECT MIN(SPORTING_EVENT_TICKET_ID), MAX(SPORTING_EVENT_TICKET_ID) FROM TICKET...
0.54	SELECT MAX(SPORTING_EVENT_TICKET_ID) FROM TICKET_PURCHASE_HIST WHERE SPORTING_EV...
0.15	DECLARE SqlDevBind1Z_1 VARCHAR2(32767):=SqlDevBind1ZInit1; SqlDevBind1Z_2 VARCH...
0.11	SELECT SUM(PURCHASE_PRICE) FROM TICKET_PURCHASE_HIST
0.08	UPDATE SPORTING_EVENT_TICKET SET TICKETHOLDER_ID = :B2 WHERE ID = :B1
0.04	SELECT * FROM SPORTING_EVENT_TICKET WHERE SPORTING_EVENT_ID = :B4 AND SEAT_LEVEL...

To learn how to see more than the default 500 bytes of SQL text, see [Accessing more SQL text in the Performance Insights dashboard \(p. 576\)](#).

A *SQL digest* is a composite of multiple actual queries that are structurally similar but might have different literal values. The digest replaces hardcoded values with a question mark. For example, a digest might be `SELECT * FROM emp WHERE lname= ?`. This digest might include the following child queries:

```
SELECT * FROM emp WHERE lname = 'Sanchez'  
SELECT * FROM emp WHERE lname = 'Olagappan'  
SELECT * FROM emp WHERE lname = 'Wu'
```

To see the literal SQL statements in a digest, select the query, and then choose the plus symbol (+). In the following example, the selected query is a digest.



Note

A SQL digest groups similar SQL statements, but doesn't redact sensitive information.

Performance Insights can show Oracle SQL text as **Unknown**. The text has this status in the following situations:

- An Oracle database user other than SYS is active but not currently executing SQL. For example, when a parallel query completes, the query coordinator waits for helper processes to send their session statistics. For the duration of the wait, the query text shows **Unknown**.
- For an RDS for Oracle instance on Standard Edition 2, Oracle Resource Manager limits the number of parallel threads. The background process doing this work causes the query text to show as **Unknown**.

SQL statistics

SQL statistics are performance-related metrics about SQL queries. For example, Performance Insights might show executions per second or rows processed per second. Performance Insights collects statistics for only the most common queries. Typically, these match the top queries by load shown in the Performance Insights dashboard.

Every line in the **Top SQL** table shows relevant statistics for the SQL statement or digest, as shown in the following example.

Top SQL		Filter sql	<	1	>	①
	Load by waits (AAS)	SQL statements		calls/sec	rows/sec	
○	0.88	select minute_rollups(?)		0.06	0.06	
○	0.53	select count(*) from authors where id < (select max(id) - 31 from authors) and ...		33.68	101.04	
○	0.17	WITH cte AS (SELECT id FROM authors LIMIT ?) UPDATE ...		33.68	33.68	
○	0.08	delete from authors where id < (select * from (select max(id) - ? from authors) ...		33.68	303.13	
○	0.07	INSERT INTO authors (id,name,email) VALUES (nextval(?),?,(nextval(?),? ,...)		33.68	303.13	
○	0.06	select count(*) from authors where id < (select max(id) - 31 from authors) and ...		0.00	0.00	

Performance Insights can report **0.00** and **- (unknown)** for SQL statistics. This situation occurs under the following conditions:

- Only one sample exists. For example, Performance Insights calculates rates of change for RDS PostgreSQL queries based on multiple samples from the pg_stats_statements view. When a workload runs for a short time, Performance Insights might collect only one sample, which means that it can't calculate a rate of change. The unknown value is represented with a dash (-).
- Two samples have the same values. Performance Insights can't calculate a rate of change because no change has occurred, so it reports the rate as **0.00**.
- An RDS PostgreSQL statement lacks a valid identifier. PostgreSQL creates a identifier for a statement only after parsing and analysis. Thus, a statement can exist in the PostgreSQL internal in-memory

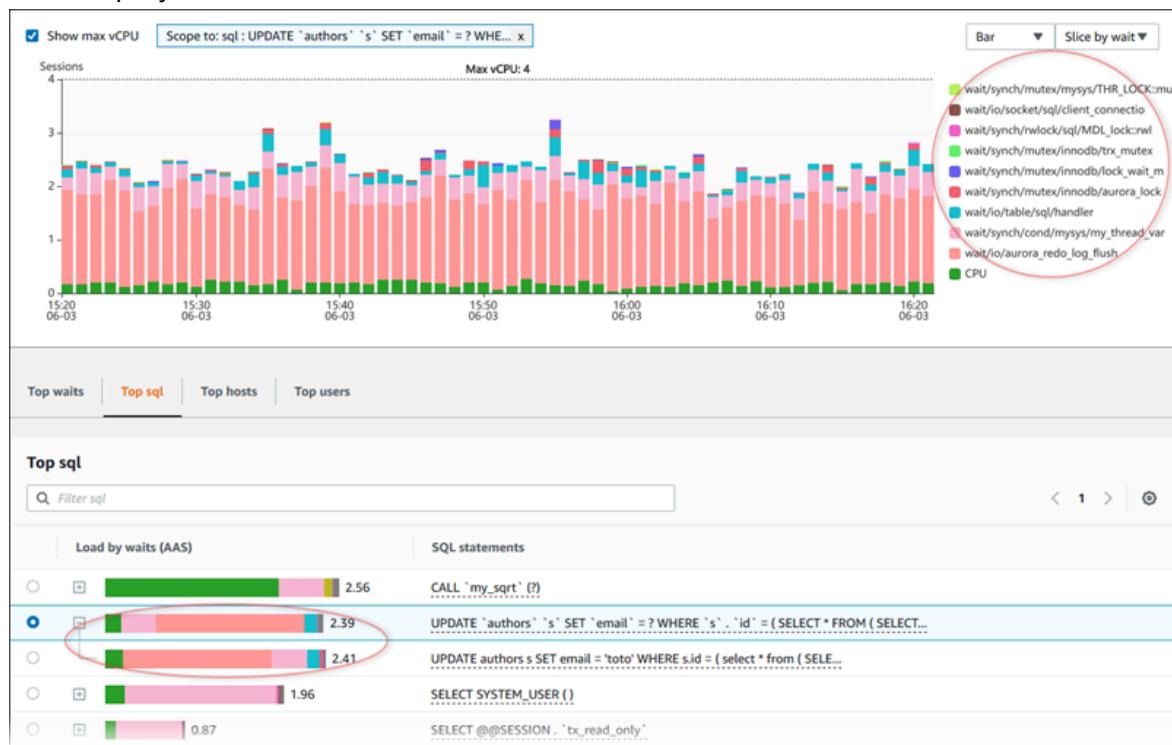
structures with no identifier. Because Performance Insights samples internal in-memory structures once per second, low-latency queries might appear for only a single sample. If the query identifier isn't available for this sample, Performance Insights can't associate this statement with its statistics. The unknown value is represented with a dash (-).

For a description of the SQL statistics for the Amazon RDS engines, see [SQL statistics for Performance Insights \(p. 628\)](#).

Load by waits (AAS)

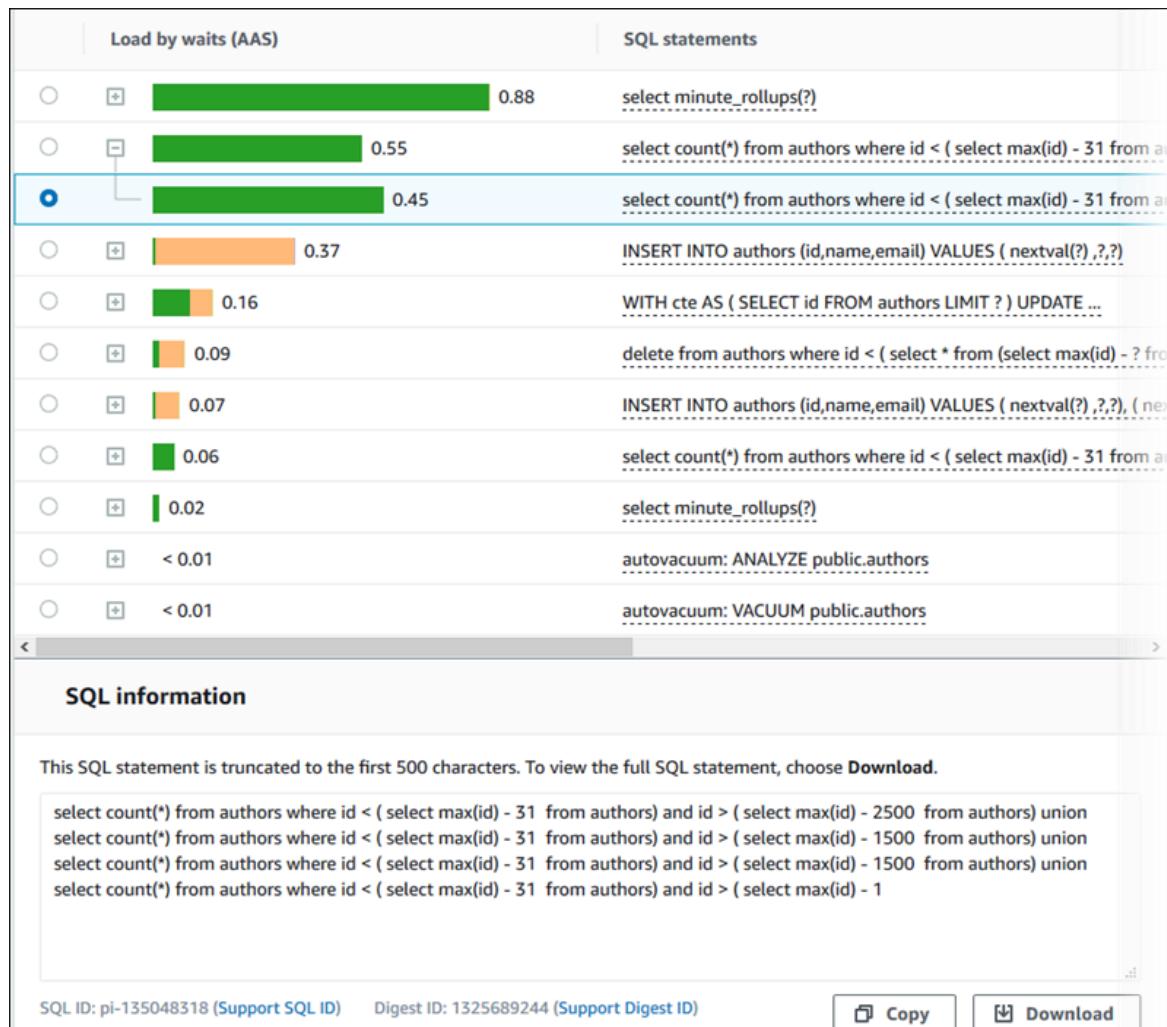
In **Top SQL**, the **Load by waits (AAS)** column illustrates the percentage of the database load associated with each top load item. This column reflects the load for that item by whatever grouping is currently selected in the **DB Load Chart**.

For example, you might group the **DB load** chart by wait states. You examine SQL queries in the top load items table. In this case, the **DB Load by Waits** bar is sized, segmented, and color-coded to show how much of a given wait state that query is contributing to. It also shows which wait states are affecting the selected query.



SQL information

In the **Top SQL** table, you can open a statement to view its information. The information appears in the bottom pane.

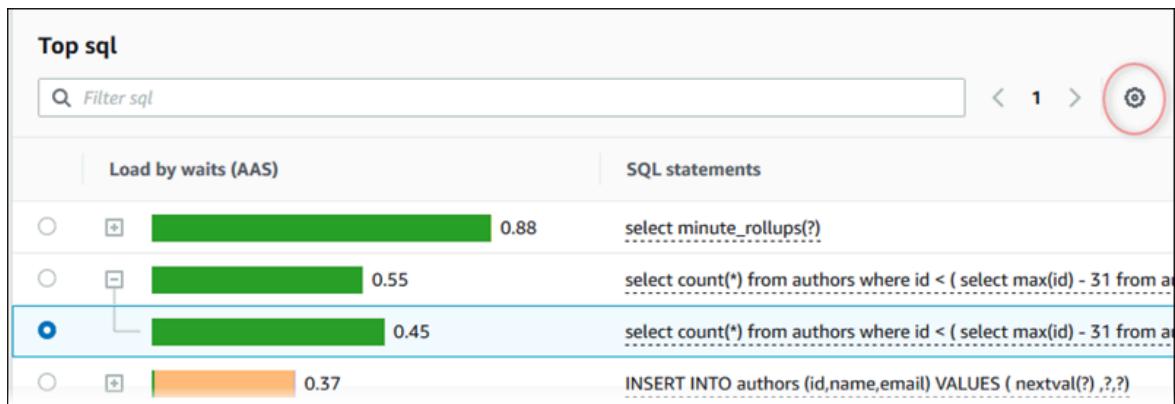


The following types of identifiers (IDs) that are associated with SQL statements:

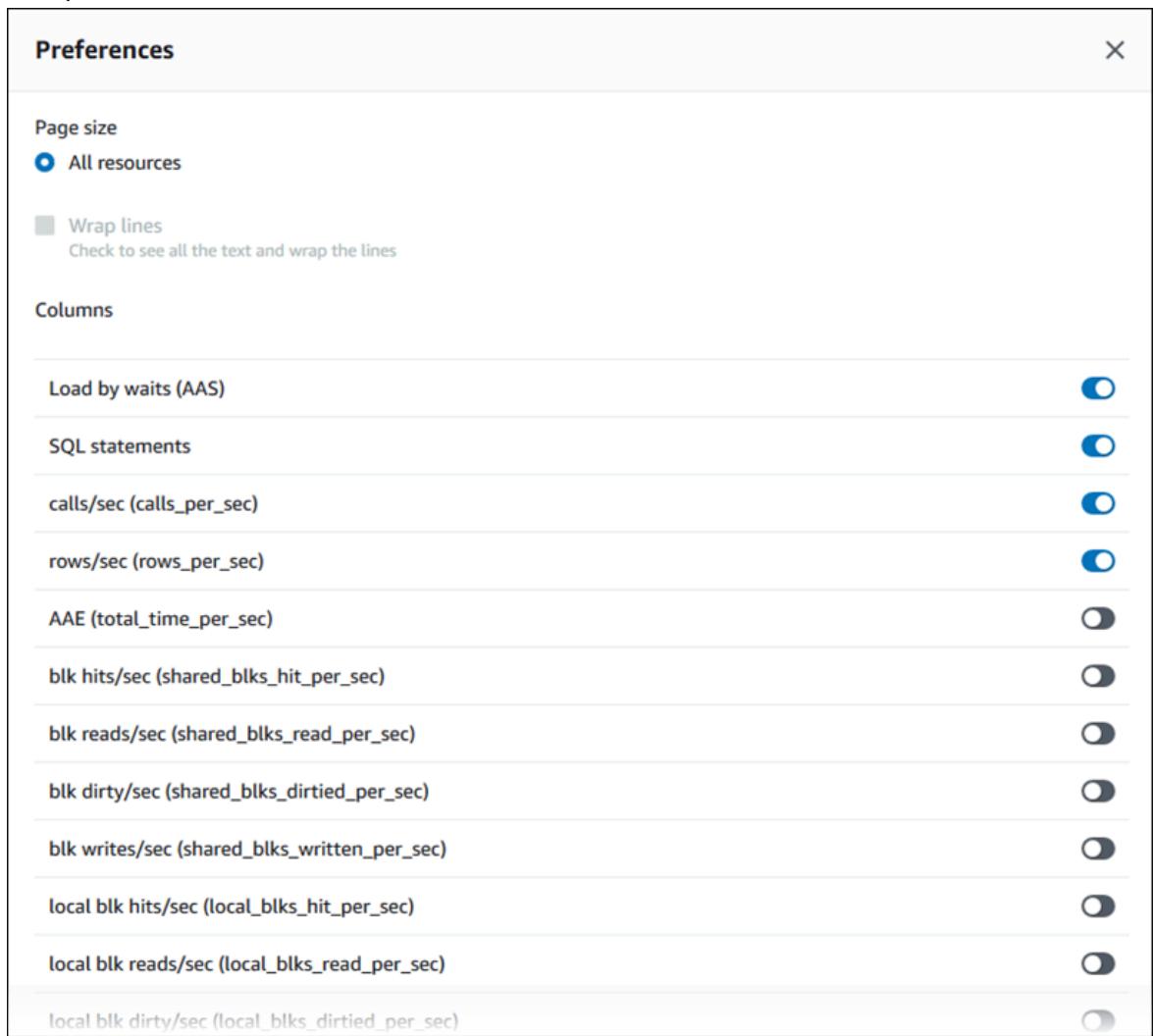
- **Support SQL ID** – A hash value of the SQL ID. This value is only for referencing a SQL ID when you are working with AWS Support. AWS Support doesn't have access to your actual SQL IDs and SQL text.
- **Support Digest ID** – A hash value of the digest ID. This value is only for referencing a digest ID when you are working with AWS Support. AWS Support doesn't have access to your actual digest IDs and SQL text.

Preferences

You can control the statistics displayed in the **Top SQL** tab by choosing the **Preferences** icon.



When you choose the **Preferences** icon, the **Preferences** window opens. The following screenshot is an example of the **Preferences** window.

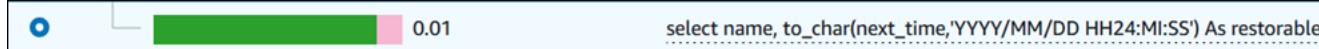


To enable the statistics that you want to appear in the **Top SQL** tab, use your mouse to scroll to the bottom of the window, and then choose **Continue**.

For more information about per-second or per-call statistics for the Amazon RDS engines, see the engine specific SQL statistics section in [SQL statistics for Performance Insights \(p. 628\)](#)

Accessing more SQL text in the Performance Insights dashboard

By default, each row in the **Top SQL** table shows 500 bytes of SQL text for each SQL statement.



When a SQL statement exceeds 500 bytes, you can view more text in the **SQL text** section below the **Top SQL** table. In this case, the maximum length for the text displayed in **SQL text** is 4 KB. This limit is introduced by the console and is subject to the limits set by the database engine. To save the text shown in **SQL text**, choose **Download**.

Topics

- [Text size limits for Amazon RDS engines \(p. 576\)](#)
- [Setting the SQL text limit for Amazon RDS for PostgreSQL DB instances \(p. 576\)](#)
- [Viewing and downloading SQL text in the Performance Insights dashboard \(p. 577\)](#)

Text size limits for Amazon RDS engines

When you download SQL text, the database engine determines its maximum length. You can download SQL text up to the following per-engine limits.

DB engine	Maximum length of downloaded text
Amazon RDS for MySQL and MariaDB	1,024 bytes
Amazon RDS for Microsoft SQL Server	4,096 characters
Amazon RDS for Oracle	1,000 bytes

The **SQL text** section of the Performance Insights console displays up to the maximum that the engine returns. For example, if MySQL returns at most 1 KB to Performance Insights, it can only collect and show 1 KB, even if the original query is larger. Thus, when you view the query in **SQL text** or download it, Performance Insights returns the same number of bytes.

If you use the AWS CLI or API, Performance Insights doesn't have the 4 KB limit enforced by the console. `DescribeDimensionKeys` and `GetResourceMetrics` return at most 500 bytes. `GetDimensionKeyDetails` returns the full query, but the size is subject to the engine limit.

Setting the SQL text limit for Amazon RDS for PostgreSQL DB instances

Amazon RDS for PostgreSQL handles text differently. You can set the text size limit with the DB instance parameter `track_activity_query_size`. This parameter has the following characteristics:

Default text size

On Amazon RDS for PostgreSQL version 9.6, the default setting for the `track_activity_query_size` parameter is 1,024 bytes. On Amazon RDS for PostgreSQL version 10 or higher, the default is 4,096 bytes.

Maximum text size

The limit for `track_activity_query_size` is 102,400 bytes for Amazon RDS for PostgreSQL version 12 and lower. The maximum is 1 MB for version 13 and higher.

If the engine returns 1 MB to Performance Insights, the console displays only the first 4 KB. If you download the query, you get the full 1 MB. In this case, viewing and downloading return different numbers of bytes. For more information about the `track_activity_query_size` DB instance parameter, see [Run-time Statistics](#) in the PostgreSQL documentation.

To increase the SQL text size, increase the `track_activity_query_size` limit. To modify the parameter, change the parameter setting in the parameter group that is associated with the Amazon RDS for PostgreSQL DB instance.

To change the setting when the instance uses the default parameter group

1. Create a new DB instance parameter group for the appropriate DB engine and DB engine version.
2. Set the parameter in the new parameter group.
3. Associate the new parameter group with the DB instance.

For information about setting a DB instance parameter, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Viewing and downloading SQL text in the Performance Insights dashboard

In the Performance Insights dashboard, you can view or download SQL text.

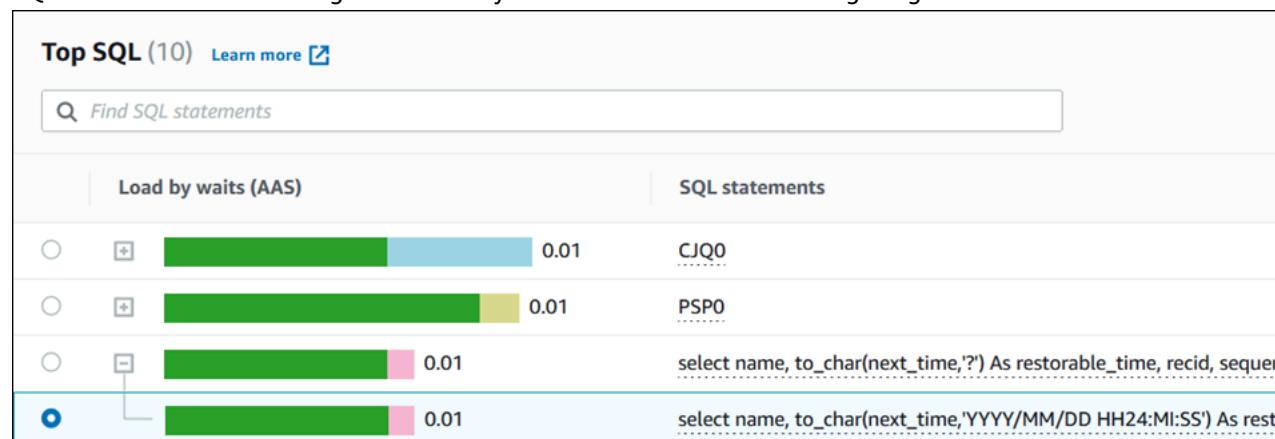
To view more SQL text in the Performance Insights dashboard

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Performance Insights**.
3. Choose a DB instance.

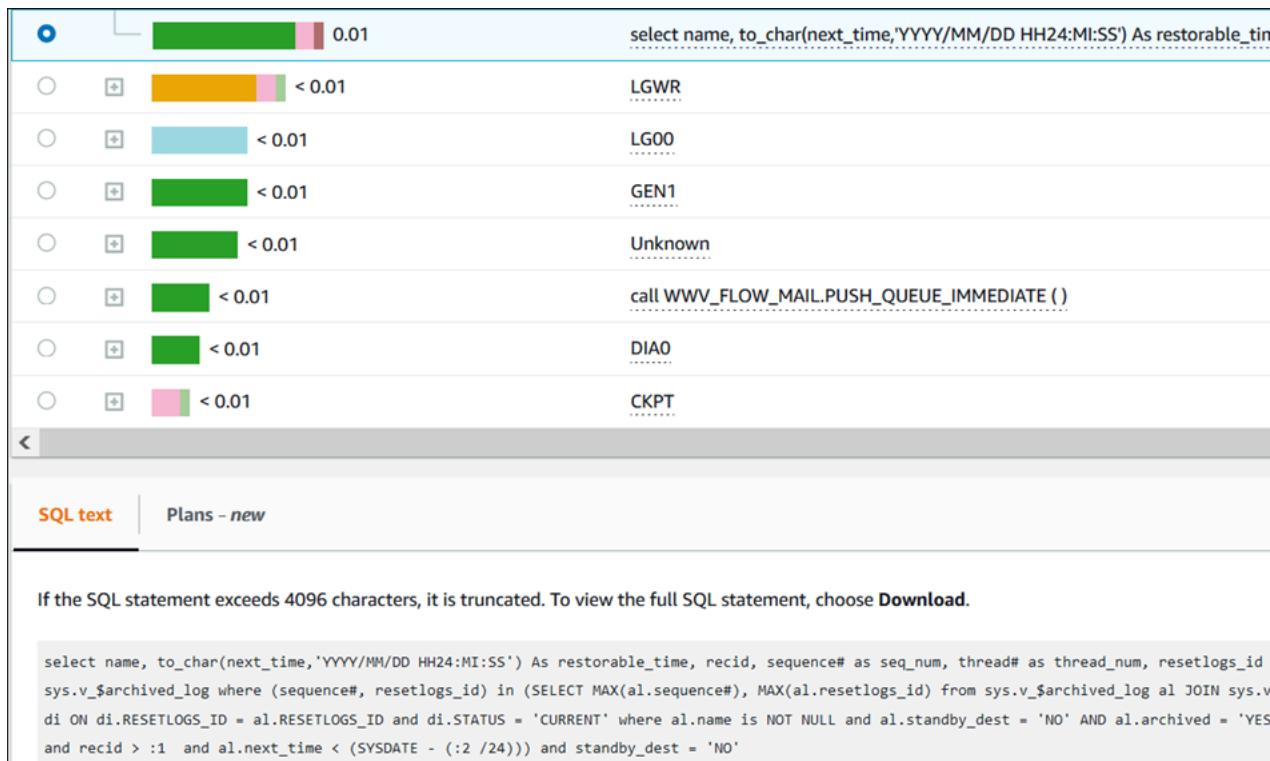
The Performance Insights dashboard is displayed for your DB instance.

4. Scroll down to the **Top SQL** tab.
5. Choose a SQL statement.

SQL statements with text larger than 500 bytes look similar to the following image.



6. Scroll down to the **SQL text** tab.



The Performance Insights dashboard can display up to 4,096 bytes for each SQL statement.

7. (Optional) Choose **Copy** to copy the displayed SQL statement, or choose **Download** to download the SQL statement to view the SQL text up to the DB engine limit.

Note

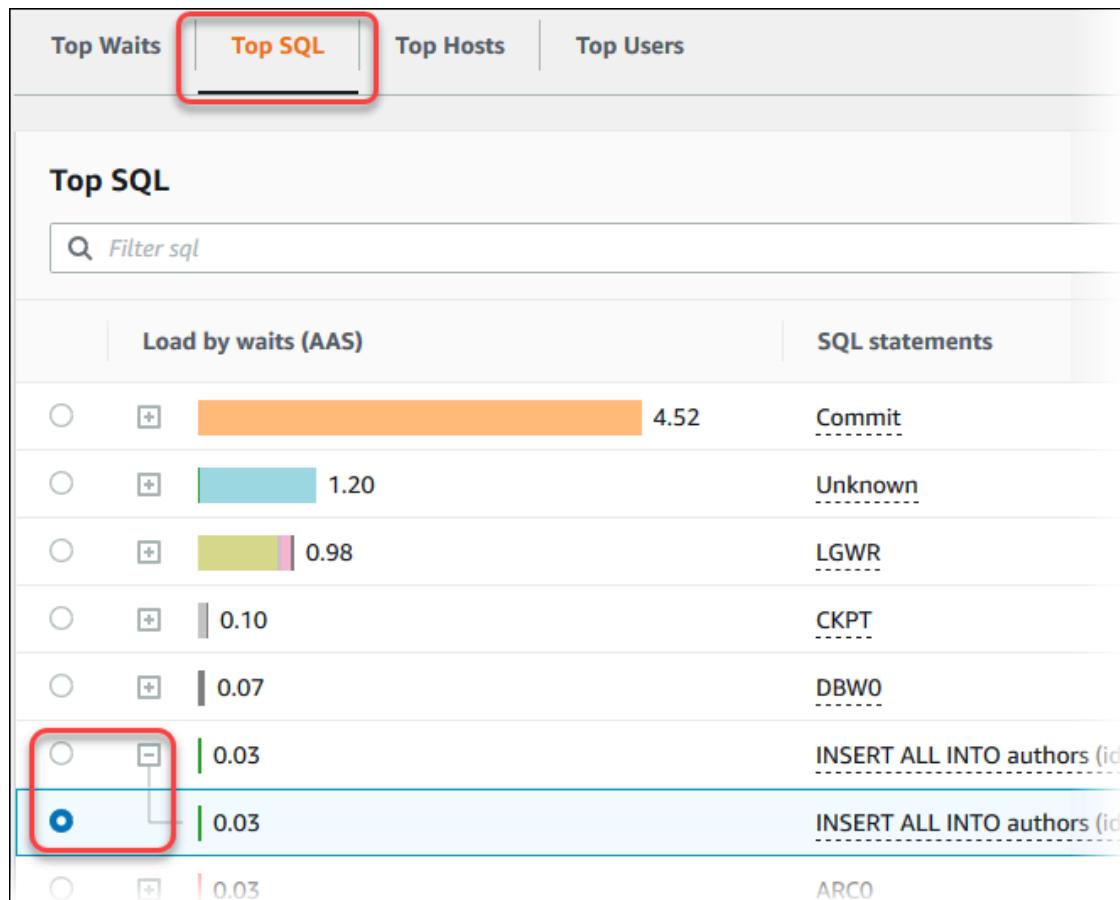
To copy or download the SQL statement, disable pop-up blockers.

Viewing SQL statistics in the Performance Insights dashboard

In the Performance Insights dashboard, SQL statistics are available in the **Top SQL** tab of the **Database load** chart.

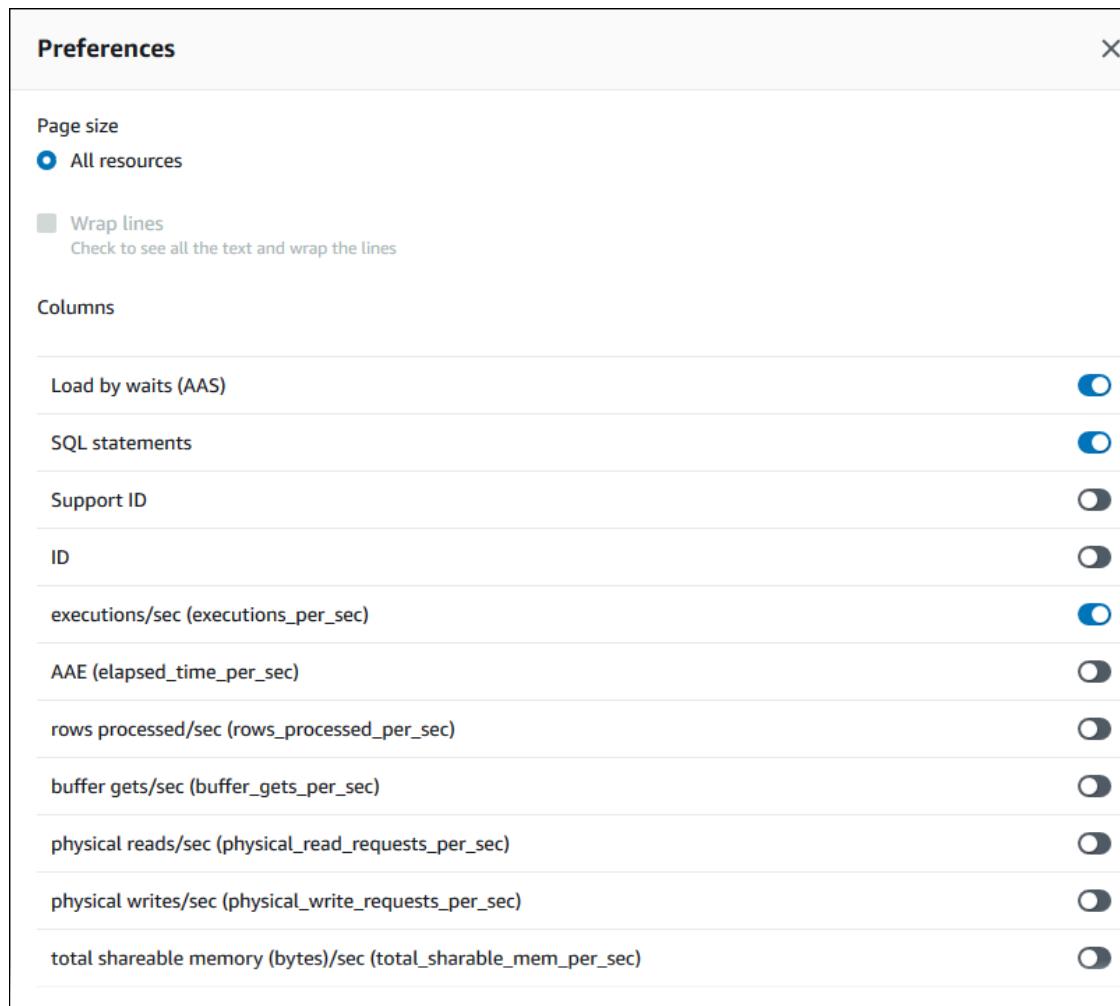
To view SQL statistics

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the left navigation pane, choose **Performance Insights**.
3. At the top of the page, choose the database whose SQL statistics you want to see.
4. Scroll to the bottom of the page and choose the **Top SQL** tab.
5. Choose an individual statement or digest query.

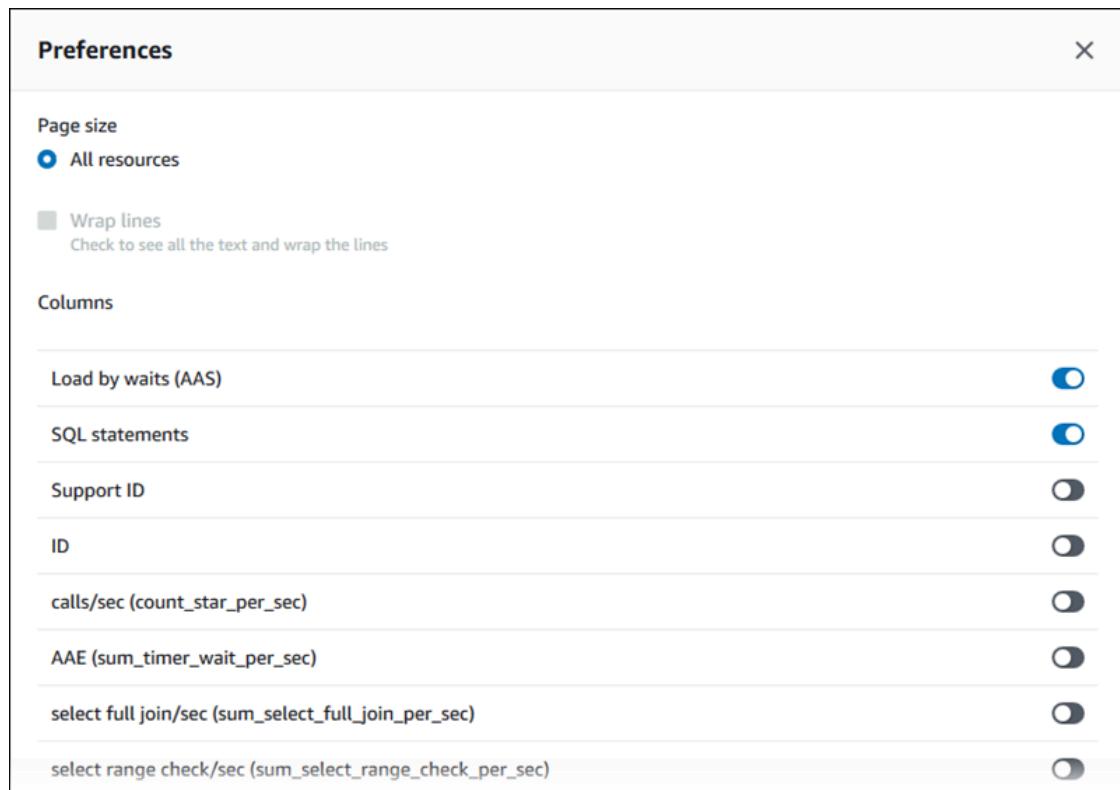


6. Choose which statistics to display by choosing the gear icon in the upper-right corner of the chart. For descriptions of the SQL statistics for the Amazon RDS engines, see [SQL statistics for Performance Insights \(p. 628\)](#).

The following example shows the statistics preferences for Oracle DB instances.



The following example shows the preferences for MariaDB and MySQL DB instances.



7. Choose Save to save your preferences.

The **Top SQL** table refreshes.

The following example shows statistics for an Oracle SQL query.

SQL statements	executions/sec	elapsed time (ms)
Commit	-	-
Unknown	-	-
LGWR	-	-
CKPT	-	-
DBWO	-	-
INSERT ALL INTO authors (id,name,email) VALUES (serial.nextval , 'Priya' , 'p@g...')	-	-
INSERT ALL INTO authors (id,name,email) VALUES (serial.nextval , 'Priya' , 'p@g...')	73.38	0.56
ARC0	-	-

Analyzing Oracle execution plans using the Performance Insights dashboard

When analyzing DB load on an Oracle Database, you might want to know which plans are contributing the most to DB load. For example, the top SQL statements at a given time might be using the plans shown in the following table.

Top SQL	Plan
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 10	Plan A
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 521	Plan B
SELECT SUM(s_total) FROM sales WHERE region = 10	Plan A
SELECT * FROM emp WHERE emp_id = 1000	Plan C
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 72	Plan A

With the plan feature of Performance Insights, you can do the following:

- Find out which plans are used by the top SQL queries.

For example, you might find out that most of the DB load is generated by queries using plan A and plan B, with only a small percentage using plan C.

- Compare different plans for the same query.

In the preceding example, three queries are identical except for the product ID. Two queries use plan A, but one query uses plan B. To see the difference in the two plans, you can use Performance Insights.

- Find out when a query switched to a new plan.

You might see that a query used plan A and then switched to plan B at a certain time. Was there a change in the database at this point? For example, if a table is empty, the optimizer might choose a full table scan. If the table is loaded with a million rows, the optimizer might switch to an index range scan.

- Drill down to the specific steps of a plan with the highest cost.

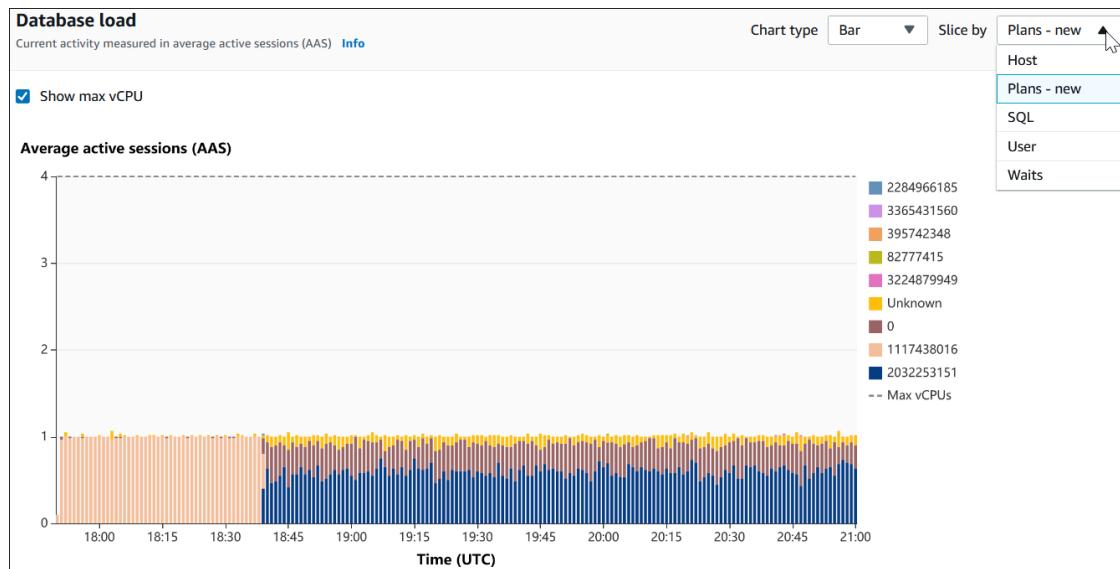
For example, the for a long-running query might show a missing a join condition in an equijoin. This missing condition forces a Cartesian join, which joins all rows of two tables.

You can perform the preceding tasks by using the plan capture feature of Performance Insights. Just as you can slice Oracle queries by wait events and top SQL, you can slice them by the plan dimension.

To analyze Oracle execution plans using the console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Performance Insights**.
3. Choose an Oracle DB instance. The Performance Insights dashboard is displayed for that DB instance.
4. In the **Database load (DB load)** section, choose **Plans** next to **Slice by**.

The Average active sessions chart shows the plans used by your top SQL statements. The plan hash values appear to the right of the color-coded squares. Each hash value uniquely identifies a plan.



5. Scroll down to the Top SQL tab.

In the following example, the top SQL digest has two plans. You can tell that it's a digest by the question mark in the statement.

Top SQL (10) Learn more				
Load by plans (AAS)		SQL statements	Execution...	Plans cou...
<input type="radio"/>	0.36	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=?	1611.28	2 plans
<input type="radio"/>	0.24	DECLARE l_output NUMBER; BEGIN while true loop FOR i IN 1..2000 LOOP ...	0.00	0 plans
<input type="radio"/>	0.02	SELECT	0.00	0 plans
<input type="radio"/>	0.02	Unknown	0.00	0 plans
<input type="radio"/>	0.01	PL/SQL EXECUTE	0.00	0 plans
<input type="radio"/>	< 0.01	PSPO	0.00	0 plans
<input type="radio"/>	< 0.01	DIAO	0.00	0 plans
<input type="radio"/>	< 0.01	CKPT	0.00	0 plans
<input type="radio"/>	< 0.01	LGWR	0.00	0 plans
<input type="radio"/>	< 0.01	SELECT /* diffdigest1469 */ count(col1) FROM tab1 WHERE col1=?	7.74	1 plans

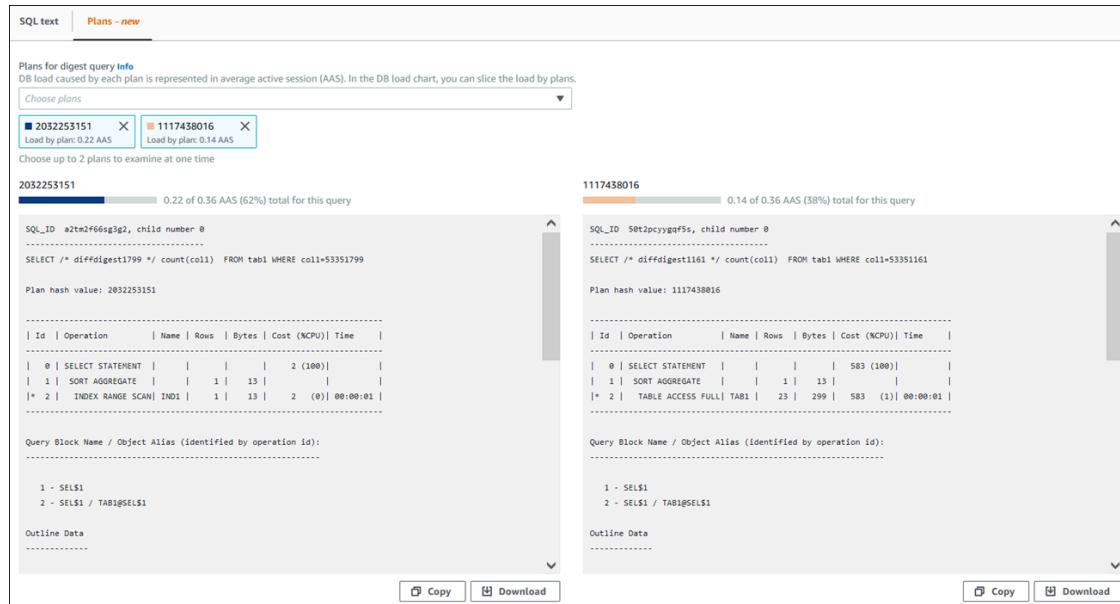
6. Choose the digest to expand it into its component statements.

In the following example, the SELECT statement is a digest query. The component queries in the digest use two different plans. The colors of the plans correspond to the database load chart. The total number of plans in the digest is shown in the second column.

Load by plans (AAS)		SQL statements	Execution...	Plans cou...
<input checked="" type="radio"/>	0.36	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=?	1611.28	2 plans
<input type="radio"/>	< 0.01	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=996827	7.43	1 plans
<input type="radio"/>	< 0.01	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=9961296	6.81	0 plans
<input type="radio"/>	< 0.01	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=996889	8.34	0 plans
<input type="radio"/>	< 0.01	SELECT /* samedigest */ count(col1) FROM tab1 WHERE col1=996503	8.67	0 plans

7. Scroll down and choose two Plans to compare from Plans for digest query list.

You can view either one or two plans for a query at a time. The following screenshot compares the two plans in the digest, with hash 2032253151 and hash 1117438016. In the following example, 62% of the average active sessions running this digest query are using the plan on the left, whereas 38% are using the plan on the right.



In this example, the plans differ in an important way. Step 2 in plan 2032253151 uses an index scan, whereas plan 1117438016 uses a full table scan. For a table with a large number of rows, a query of a single row is almost always faster with an index scan.



8. (Optional) Choose **Copy** to copy the plan to the clipboard, or **Download** to save the plan to your hard drive.

Retrieving metrics with the Performance Insights API

When Performance Insights is enabled, the API provides visibility into instance performance. Amazon CloudWatch Logs provides the authoritative source for vended monitoring metrics for AWS services.

Performance Insights offers a domain-specific view of database load measured as average active sessions (AAS). This metric appears to API consumers as a two-dimensional time-series dataset. The time dimension of the data provides DB load data for each time point in the queried time range. Each time point decomposes overall load in relation to the requested dimensions, such as SQL, Wait-event, User, or Host, measured at that time point.

Amazon RDS Performance Insights monitors your Amazon RDS DB instance so that you can analyze and troubleshoot database performance. One way to view Performance Insights data is in the AWS Management Console. Performance Insights also provides a public API so that you can query your own data. You can use the API to do the following:

- Offload data into a database
- Add Performance Insights data to existing monitoring dashboards
- Build monitoring tools

To use the Performance Insights API, enable Performance Insights on one of your Amazon RDS DB instances. For information about enabling Performance Insights, see [Turning Performance Insights on and off \(p. 549\)](#). For more information about the Performance Insights API, see the [Amazon RDS Performance Insights API Reference](#).

The Performance Insights API provides the following operations.

Performance Insights action	AWS CLI command	Description
DescribeDimensionKeys	<code>aws pi describe-dimension-keys</code>	Retrieves the top N dimension keys for a metric for a specific time period.
GetDimensionKeyDetails	<code>aws pi get-dimension-key-details</code>	Retrieves the attributes of the specified dimension group for a DB instance or data source. For example, if you specify a SQL ID, and if the dimension details are available, <code>GetDimensionKeyDetails</code> retrieves the full text of the dimension <code>db.sql.statement</code> associated with this ID. This operation is useful because <code>GetResourceMetrics</code> and <code>DescribeDimensionKeys</code> don't support retrieval of large SQL statement text.
GetResourceMetadata	<code>aws pi get-resource-metadata</code>	Retrieve the metadata for different features. For example, the metadata might indicate that a feature is turned on or off on a specific DB instance.
GetResourceMetrics	<code>aws pi get-resource-metrics</code>	Retrieves Performance Insights metrics for a set of data sources over a time period. You can provide specific dimension groups and dimensions, and provide aggregation and filtering criteria for each group.
ListAvailableResourceDimensions	<code>aws pi list-available-resource-dimensions</code>	Retrieve the dimensions that can be queried for each specified metric type on a specified instance.
ListAvailableResourceMetrics	<code>aws pi list-available-resource-metrics</code>	Retrieve all available metrics of the specified metric types that can be queried for a specified DB instance.

Topics

- [AWS CLI for Performance Insights \(p. 586\)](#)
- [Retrieving time-series metrics \(p. 586\)](#)
- [AWS CLI examples for Performance Insights \(p. 587\)](#)

AWS CLI for Performance Insights

You can view Performance Insights data using the AWS CLI. You can view help for the AWS CLI commands for Performance Insights by entering the following on the command line.

```
aws pi help
```

If you don't have the AWS CLI installed, see [Installing the AWS Command Line Interface](#) in the *AWS CLI User Guide* for information about installing it.

Retrieving time-series metrics

The `GetResourceMetrics` operation retrieves one or more time-series metrics from the Performance Insights data. `GetResourceMetrics` requires a metric and time period, and returns a response with a list of data points.

For example, the AWS Management Console uses `GetResourceMetrics` to populate the **Counter Metrics** chart and the **Database Load** chart, as seen in the following image.



All metrics returned by `GetResourceMetrics` are standard time-series metrics, with the exception of `db.load`. This metric is displayed in the **Database Load** chart. The `db.load` metric is different from the other time-series metrics because you can break it into subcomponents called *dimensions*. In the previous image, `db.load` is broken down and grouped by the waits states that make up the `db.load`.

Note

`GetResourceMetrics` can also return the `db.sampleload` metric, but the `db.load` metric is appropriate in most cases.

For information about the counter metrics returned by `GetResourceMetrics`, see [Performance Insights counter metrics \(p. 618\)](#).

The following calculations are supported for the metrics:

- Average – The average value for the metric over a period of time. Append `.avg` to the metric name.
- Minimum – The minimum value for the metric over a period of time. Append `.min` to the metric name.
- Maximum – The maximum value for the metric over a period of time. Append `.max` to the metric name.
- Sum – The sum of the metric values over a period of time. Append `.sum` to the metric name.
- Sample count – The number of times the metric was collected over a period of time. Append `.sample_count` to the metric name.

For example, assume that a metric is collected for 300 seconds (5 minutes), and that the metric is collected one time each minute. The values for each minute are 1, 2, 3, 4, and 5. In this case, the following calculations are returned:

- Average – 3
- Minimum – 1
- Maximum – 5
- Sum – 15
- Sample count – 5

For information about using the `get-resource-metrics` AWS CLI command, see [get-resource-metrics](#).

For the `--metric-queries` option, specify one or more queries that you want to get results for. Each query consists of a mandatory `Metric` and optional `GroupBy` and `Filter` parameters. The following is an example of a `--metric-queries` option specification.

```
{  
    "Metric": "string",  
    "GroupBy": {  
        "Group": "string",  
        "Dimensions": ["string", ...],  
        "Limit": integer  
    },  
    "Filter": {"string": "string"  
    ...}
```

AWS CLI examples for Performance Insights

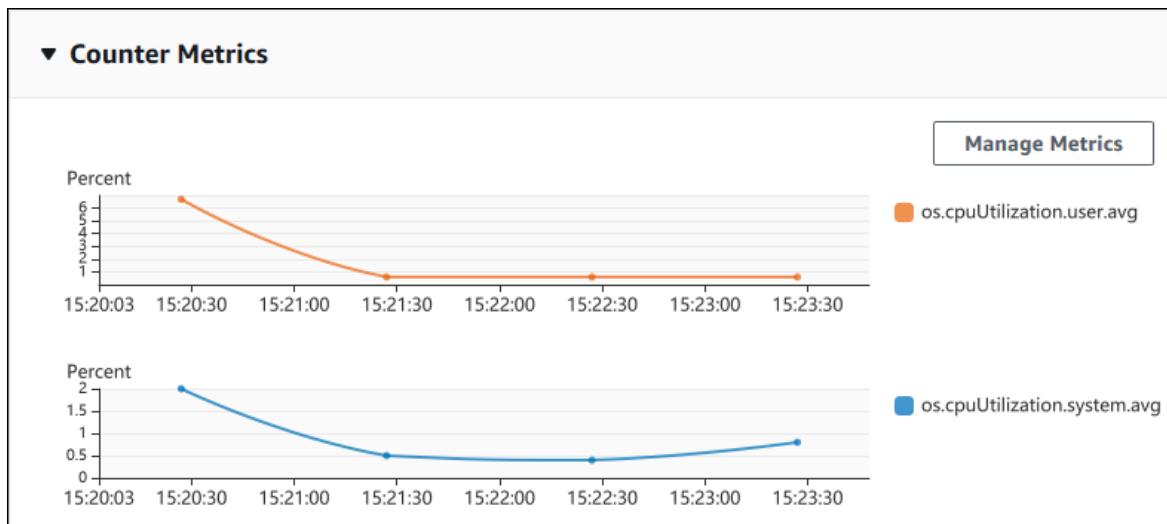
The following examples show how to use the AWS CLI for Performance Insights.

Topics

- [Retrieving counter metrics \(p. 587\)](#)
- [Retrieving the DB load average for top wait events \(p. 590\)](#)
- [Retrieving the DB load average for top SQL \(p. 592\)](#)
- [Retrieving the DB load average filtered by SQL \(p. 594\)](#)
- [Retrieving the full text of a SQL statement \(p. 597\)](#)

Retrieving counter metrics

The following screenshot shows two counter metrics charts in the AWS Management Console.



The following example shows how to gather the same data that the AWS Management Console uses to generate the two counter metric charts.

For Linux, macOS, or Unix:

```
aws pi get-resource-metrics \
--service-type RDS \
--identifier db-ID \
--start-time 2018-10-30T00:00:00Z \
--end-time 2018-10-30T01:00:00Z \
--period-in-seconds 60 \
--metric-queries '[{"Metric": "os.cpuUtilization.user.avg"}, {"Metric": "os.cpuUtilization.idle.avg"}]'
```

For Windows:

```
aws pi get-resource-metrics ^
--service-type RDS ^
--identifier db-ID ^
--start-time 2018-10-30T00:00:00Z ^
--end-time 2018-10-30T01:00:00Z ^
--period-in-seconds 60 ^
--metric-queries '[{"Metric": "os.cpuUtilization.user.avg"}, {"Metric": "os.cpuUtilization.idle.avg"}]'
```

You can also make a command easier to read by specifying a file for the `--metrics-query` option. The following example uses a file called `query.json` for the option. The file has the following contents.

```
[  
  {  
    "Metric": "os.cpuUtilization.user.avg"  
  },  
  {  
    "Metric": "os.cpuUtilization.idle.avg"  
  }]
```

Run the following command to use the file.

For Linux, macOS, or Unix:

```
aws pi get-resource-metrics \
--service-type RDS \
--identifier db-ID \
--start-time 2018-10-30T00:00:00Z \
--end-time 2018-10-30T01:00:00Z \
--period-in-seconds 60 \
--metric-queries file://query.json
```

For Windows:

```
aws pi get-resource-metrics ^
--service-type RDS ^
--identifier db-ID ^
--start-time 2018-10-30T00:00:00Z ^
--end-time 2018-10-30T01:00:00Z ^
--period-in-seconds 60 ^
--metric-queries file://query.json
```

The preceding example specifies the following values for the options:

- **--service-type** – RDS for Amazon RDS
- **--identifier** – The resource ID for the DB instance
- **--start-time** and **--end-time** – The ISO 8601 DateTime values for the period to query, with multiple supported formats

It queries for a one-hour time range:

- **--period-in-seconds** – 60 for a per-minute query
- **--metric-queries** – An array of two queries, each just for one metric.

The metric name uses dots to classify the metric in a useful category, with the final element being a function. In the example, the function is avg for each query. As with Amazon CloudWatch, the supported functions are min, max, total, and avg.

The response looks similar to the following.

```
{
  "Identifier": "db-XXX",
  "AlignedStartTime": 1540857600.0,
  "AlignedEndTime": 1540861200.0,
  "MetricList": [
    { //A list of key/datapoints
      "Key": {
        "Metric": "os.cpuUtilization.user.avg" //Metric1
      },
      "DataPoints": [
        //Each list of datapoints has the same timestamps and same number of items
        {
          "Timestamp": 1540857660.0, //Minute1
          "Value": 4.0
        },
        {
          "Timestamp": 1540857720.0, //Minute2
          "Value": 4.0
        },
        {
          "Timestamp": 1540857780.0, //Minute 3
          "Value": 10.0
        }
      ]
    }
  ]
}
```

```

        }
        //... 60 datapoints for the os.cpuUtilization.user.avg metric
    ],
    {
        "Key": {
            "Metric": "os.cpuUtilization.idle.avg" //Metric2
        },
        "DataPoints": [
            {
                "Timestamp": 1540857660.0, //Minute1
                "Value": 12.0
            },
            {
                "Timestamp": 1540857720.0, //Minute2
                "Value": 13.5
            },
            //... 60 datapoints for the os.cpuUtilization.idle.avg metric
        ]
    }
] //end of MetricList
} //end of response

```

The response has an `Identifier`, `AlignedStartTime`, and `AlignedEndTime`. Because the `--period-in-seconds` value was 60, the start and end times have been aligned to the minute. If the `--period-in-seconds` was 3600, the start and end times would have been aligned to the hour.

The `MetricList` in the response has a number of entries, each with a `Key` and a `DataPoints` entry. Each `DataPoint` has a `Timestamp` and a `Value`. Each `DataPoints` list has 60 data points because the queries are for per-minute data over an hour, with `Timestamp1/Minute1`, `Timestamp2/Minute2`, and so on, up to `Timestamp60/Minute60`.

Because the query is for two different counter metrics, there are two elements in the response `MetricList`.

Retrieving the DB load average for top wait events

The following example is the same query that the AWS Management Console uses to generate a stacked area line graph. This example retrieves the `db.load.avg` for the last hour with load divided according to the top seven wait events. The command is the same as the command in [Retrieving counter metrics \(p. 587\)](#). However, the `query.json` file has the following contents.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 7 }
    }
]
```

Run the following command.

For Linux, macOS, or Unix:

```
aws pi get-resource-metrics \
--service-type RDS \
--identifier db-ID \
--start-time 2018-10-30T00:00:00Z \
--end-time 2018-10-30T01:00:00Z \
--period-in-seconds 60 \
--metric-queries file://query.json
```

For Windows:

```
aws pi get-resource-metrics ^
--service-type RDS ^
--identifier db-ID ^
--start-time 2018-10-30T00:00:00Z ^
--end-time 2018-10-30T01:00:00Z ^
--period-in-seconds 60 ^
--metric-queries file://query.json
```

The example specifies the metric of db.load.avg and a GroupBy of the top seven wait events. For details about valid values for this example, see [DimensionGroup](#) in the *Performance Insights API Reference*.

The response looks similar to the following.

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1540857600.0,
    "AlignedEndTime": 1540861200.0,
    "MetricList": [
        { //A list of key/datapoints
            "Key": {
                //A Metric with no dimensions. This is the total db.load.avg
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of items
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.5166666666666667
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.3833333333333336
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
                    "Value": 0.2666666666666666
                }
                //... 60 datapoints for the total db.load.avg key
            ]
        },
        {
            "Key": {
                //Another key. This is db.load.avg broken down by CPU
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.name": "CPU",
                    "db.wait_event.type": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.35
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.15
                },
                //... 60 datapoints for the CPU key
            ]
        },
    ],
}
```

```
//... In total we have 8 key/datapoints entries, 1) total, 2-8) Top Wait Events
] //end of MetricList
} //end of response
```

In this response, there are eight entries in the MetricList. There is one entry for the total db.load.avg, and seven entries each for the db.load.avg divided according to one of the top seven wait events. Unlike in the first example, because there was a grouping dimension, there must be one key for each grouping of the metric. There can't be only one key for each metric, as in the basic counter metric use case.

Retrieving the DB load average for top SQL

The following example groups db.wait_events by the top 10 SQL statements. There are two different groups for SQL statements:

- db.sql – The full SQL statement, such as `select * from customers where customer_id = 123`
- db.sql_tokenized – The tokenized SQL statement, such as `select * from customers where customer_id = ?`

When analyzing database performance, it can be useful to consider SQL statements that only differ by their parameters as one logic item. So, you can use db.sql_tokenized when querying. However, especially when you're interested in explain plans, sometimes it's more useful to examine full SQL statements with parameters, and query grouping by db.sql. There is a parent-child relationship between tokenized and full SQL, with multiple full SQL (children) grouped under the same tokenized SQL (parent).

The command in this example is the similar to the command in [Retrieving the DB load average for top wait events \(p. 590\)](#). However, the query.json file has the following contents.

```
[  
  {  
    "Metric": "db.load.avg",  
    "GroupBy": { "Group": "db.sql_tokenized", "Limit": 10 }  
  }  
]
```

The following example uses db.sql_tokenized.

For Linux, macOS, or Unix:

```
aws pi get-resource-metrics \  
  --service-type RDS \  
  --identifier db-ID \  
  --start-time 2018-10-29T00:00:00Z \  
  --end-time 2018-10-30T00:00:00Z \  
  --period-in-seconds 3600 \  
  --metric-queries file://query.json
```

For Windows:

```
aws pi get-resource-metrics ^  
  --service-type RDS ^  
  --identifier db-ID ^  
  --start-time 2018-10-29T00:00:00Z ^  
  --end-time 2018-10-30T00:00:00Z ^
```

```
--period-in-seconds 3600 ^
--metric-queries file:///query.json
```

This example queries over 24 hours, with a one hour period-in-seconds.

The example specifies the metric of db.load.avg and a GroupBy of the top seven wait events. For details about valid values for this example, see [DimensionGroup](#) in the *Performance Insights API Reference*.

The response looks similar to the following.

```
{
    "AlignedStartTime": 1540771200.0,
    "AlignedEndTime": 1540857600.0,
    "Identifier": "db-XXX",

    "MetricList": [ //11 entries in the MetricList
        {
            "Key": { //First key is total
                "Metric": "db.load.avg"
            }
            "DataPoints": [ //Each DataPoints list has 24 per-hour Timestamps and a value
                {
                    "Value": 1.6964980544747081,
                    "Timestamp": 1540774800.0
                },
                //... 24 datapoints
            ]
        },
        {
            "Key": { //Next key is the top tokenized SQL
                "Dimensions": {
                    "db.sql_tokenized.statement": "INSERT INTO authors (id,name,email)
VALUES\n( nextval(?) ,?,?)",
                    "db.sql_tokenized.db_id": "pi-2372568224",
                    "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE"
                },
                "Metric": "db.load.avg"
            },
            "DataPoints": [ //... 24 datapoints
            ]
        },
        // In total 11 entries, 10 Keys of top tokenized SQL, 1 total key
    ] //End of MetricList
} //End of response
```

This response has 11 entries in the MetricList (1 total, 10 top tokenized SQL), with each entry having 24 per-hour DataPoints.

For tokenized SQL, there are three entries in each dimensions list:

- db.sql_tokenized.statement – The tokenized SQL statement.
- db.sql_tokenized.db_id – Either the native database ID used to refer to the SQL, or a synthetic ID that Performance Insights generates for you if the native database ID isn't available. This example returns the pi-2372568224 synthetic ID.
- db.sql_tokenized.id – The ID of the query inside Performance Insights.

In the AWS Management Console, this ID is called the Support ID. It's named this because the ID is data that AWS Support can examine to help you troubleshoot an issue with your database. AWS takes the security and privacy of your data extremely seriously, and almost all data is stored encrypted with your AWS KMS customer master key (CMK). Therefore, nobody inside AWS can look at this data. In

In the example preceding, both the `tokenized.statement` and the `tokenized.db_id` are stored encrypted. If you have an issue with your database, AWS Support can help you by referencing the Support ID.

When querying, it might be convenient to specify a Group in `GroupBy`. However, for finer-grained control over the data that's returned, specify the list of dimensions. For example, if all that is needed is the `db.sql_tokenized.statement`, then a `Dimensions` attribute can be added to the `query.json` file.

```
[  
  {  
    "Metric": "db.load.avg",  
    "GroupBy": {  
      "Group": "db.sql_tokenized",  
      "Dimensions": ["db.sql_tokenized.statement"],  
      "Limit": 10  
    }  
  }  
]
```

Retrieving the DB load average filtered by SQL



The preceding image shows that a particular query is selected, and the top average active sessions stacked area line graph is scoped to that query. Although the query is still for the top seven overall wait events, the value of the response is filtered. The filter causes it to take into account only sessions that are a match for the particular filter.

The corresponding API query in this example is similar to the command in [Retrieving the DB load average for top SQL \(p. 592\)](#). However, the `query.json` file has the following contents.

```
[  
  {  
    "Metric": "db.load.avg",  
    "GroupBy": { "Group": "db.wait_event", "Limit": 5 },  
    "Filter": { "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }  
}
```

]

For Linux, macOS, or Unix:

```
aws pi get-resource-metrics \
--service-type RDS \
--identifier db-ID \
--start-time 2018-10-30T00:00:00Z \
--end-time 2018-10-30T01:00:00Z \
--period-in-seconds 60 \
--metric-queries file://query.json
```

For Windows:

```
aws pi get-resource-metrics ^
--service-type RDS ^
--identifier db-ID ^
--start-time 2018-10-30T00:00:00Z ^
--end-time 2018-10-30T01:00:00Z ^
--period-in-seconds 60 ^
--metric-queries file://query.json
```

The response looks similar to the following.

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1556215200.0,
    "MetricList": [
        {
            "Key": {
                "Metric": "db.load.avg"
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.4878117913832196
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.192823803967328
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "io",
                    "db.wait_event.name": "wait/io/aurora_redo_log_flush"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.1360544217687074
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.058051341890315
                }
            ]
        },
    ],
}
```

```
{
    "Key": {
        "Metric": "db.load.avg",
        "Dimensions": {
            "db.wait_event.type": "io",
            "db.wait_event.name": "wait/io/table/sql/handler"
        }
    },
    "DataPoints": [
        {
            "Timestamp": 1556218800.0,
            "Value": 0.16241496598639457
        },
        {
            "Timestamp": 1556222400.0,
            "Value": 0.05163360560093349
        }
    ]
},
{
    "Key": {
        "Metric": "db.load.avg",
        "Dimensions": {
            "db.wait_event.type": "synch",
            "db.wait_event.name": "wait/synch/mutex/innodb/aurora_lock_thread_slot_futex"
        }
    },
    "DataPoints": [
        {
            "Timestamp": 1556218800.0,
            "Value": 0.11479591836734694
        },
        {
            "Timestamp": 1556222400.0,
            "Value": 0.013127187864644107
        }
    ]
},
{
    "Key": {
        "Metric": "db.load.avg",
        "Dimensions": {
            "db.wait_event.type": "CPU",
            "db.wait_event.name": "CPU"
        }
    },
    "DataPoints": [
        {
            "Timestamp": 1556218800.0,
            "Value": 0.05215419501133787
        },
        {
            "Timestamp": 1556222400.0,
            "Value": 0.05805134189031505
        }
    ]
},
{
    "Key": {
        "Metric": "db.load.avg",
        "Dimensions": {
            "db.wait_event.type": "synch",
            "db.wait_event.name": "wait/synch/mutex/innodb/lock_wait_mutex"
        }
    },
}
```

```

    "DataPoints": [
      {
        "Timestamp": 1556218800.0,
        "Value": 0.017573696145124718
      },
      {
        "Timestamp": 1556222400.0,
        "Value": 0.002333722287047841
      }
    ]
  ],
  "AlignedEndTime": 1556222400.0
} //end of response

```

In this response, all values are filtered according to the contribution of tokenized SQL AKIAIOSFODNN7EXAMPLE specified in the query.json file. The keys also might follow a different order than a query without a filter, because it's the top five wait events that affected the filtered SQL.

Retrieving the full text of a SQL statement

The following example retrieves the full text of a SQL statement for DB instance db-10BCD2EFGHIJ3KL4M5N06PQRS5. The --group is db.sql, and the --group-identifier is db.sql.id. In this example, *my-sql-id* represents a SQL ID retrieved by invoking pi get-resource-metrics or pi describe-dimension-keys.

Run the following command.

For Linux, macOS, or Unix:

```

aws pi get-dimension-key-details \
--service-type RDS \
--identifier db-10BCD2EFGHIJ3KL4M5N06PQRS5 \
--group db.sql \
--group-identifier my-sql-id \
--requested-dimensions statement

```

For Windows:

```

aws pi get-dimension-key-details ^
--service-type RDS ^
--identifier db-10BCD2EFGHIJ3KL4M5N06PQRS5 ^
--group db.sql ^
--group-identifier my-sql-id ^
--requested-dimensions statement

```

In this example, the dimensions details are available. Thus, Performance Insights retrieves the full text of the SQL statement, without truncating it.

```

{
  "Dimensions": [
    {
      "Value": "SELECT e.last_name, d.department_name FROM employees e, departments d
WHERE e.department_id=d.department_id",
      "Dimension": "db.sql.statement",
      "Status": "AVAILABLE"
    },
    ...
  ]
}

```

}

Logging Performance Insights calls using AWS CloudTrail

Performance Insights runs with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Performance Insights. CloudTrail captures all API calls for Performance Insights as events. This capture includes calls from the Amazon RDS console and from code calls to the Performance Insights API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Performance Insights. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the data collected by CloudTrail, you can determine certain information. This information includes the request that was made to Performance Insights, the IP address the request was made from, who made the request, and when it was made. It also includes additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

Working with Performance Insights information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Performance Insights, that activity is recorded in a CloudTrail event along with other AWS service events in the CloudTrail console in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing Events with CloudTrail Event History](#) in *AWS CloudTrail User Guide*.

For an ongoing record of events in your AWS account, including events for Performance Insights, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following topics in *AWS CloudTrail User Guide*:

- [Overview for Creating a Trail](#)
- [CloudTrail Supported Services and Integrations](#)
- [Configuring Amazon SNS Notifications for CloudTrail](#)
- [Receiving CloudTrail Log Files from Multiple Regions](#) and [Receiving CloudTrail Log Files from Multiple Accounts](#)

All Performance Insights operations are logged by CloudTrail and are documented in the [Performance Insights API Reference](#). For example, calls to the `DescribeDimensionKeys` and `GetResourceMetrics` operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail userIdentity Element](#).

Performance Insights log file entries

A *trail* is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An *event* represents a single request from any source. Each event includes information about the requested operation, the date and time of the operation, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `GetResourceMetrics` operation.

```
{  
    "eventVersion": "1.05",  
    "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "AKIAIOSFODNN7EXAMPLE",  
        "arn": "arn:aws:iam::123456789012:user/johndoe",  
        "accountId": "123456789012",  
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",  
        "userName": "johndoe"  
    },  
    "eventTime": "2019-12-18T19:28:46Z",  
    "eventSource": "pi.amazonaws.com",  
    "eventName": "GetResourceMetrics",  
    "awsRegion": "us-east-1",  
    "sourceIPAddress": "72.21.198.67",  
    "userAgent": "aws-cli/1.16.240 Python/3.7.4 Darwin/18.7.0 botocore/1.12.230",  
    "requestParameters": {  
        "identifier": "db-YTDU5J5V66X7CXSCVDFD2V3SZM",  
        "metricQueries": [  
            {  
                "metric": "os.cpuUtilization.user.avg"  
            },  
            {  
                "metric": "os.cpuUtilization.idle.avg"  
            }  
        ],  
        "startTime": "Dec 18, 2019 5:28:46 PM",  
        "periodInSeconds": 60,  
        "endTime": "Dec 18, 2019 7:28:46 PM",  
        "serviceType": "RDS"  
    },  
    "responseElements": null,  
    "requestID": "9ffbe15c-96b5-4fe6-bed9-9fccff1a0525",  
    "eventID": "08908de0-2431-4e2e-ba7b-f5424f908433",  
    "eventType": "AwsApiCall",  
    "recipientAccountId": "123456789012"  
}
```

Monitoring OS metrics with Enhanced Monitoring

With Enhanced Monitoring, you can monitor the operating system of your DB instance in real time. When you want to see how different processes or threads use the CPU, Enhanced Monitoring metrics are useful.

Topics

- [Overview of Enhanced Monitoring \(p. 600\)](#)
- [Setting up and enabling Enhanced Monitoring \(p. 601\)](#)
- [Viewing OS metrics in the RDS console \(p. 605\)](#)
- [Viewing OS metrics using CloudWatch Logs \(p. 608\)](#)

Overview of Enhanced Monitoring

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view all the system metrics and process information for your RDS DB instances on the console. You can manage which metrics you want to monitor for each instance and customize the dashboard according to your requirements. For descriptions of the Enhanced Monitoring metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#).

RDS delivers the metrics from Enhanced Monitoring into your Amazon CloudWatch Logs account. You can create metrics filters in CloudWatch from CloudWatch Logs and display the graphs on the CloudWatch dashboard. You can consume the Enhanced Monitoring JSON output from CloudWatch Logs in a monitoring system of your choice. For more information, see [Enhanced Monitoring](#) in the Amazon RDS FAQs.

Topics

- [Enhanced Monitoring availability \(p. 600\)](#)
- [Differences between CloudWatch and Enhanced Monitoring metrics \(p. 600\)](#)
- [Retention of Enhanced Monitoring metrics \(p. 601\)](#)
- [Cost of Enhanced Monitoring \(p. 601\)](#)

Enhanced Monitoring availability

Enhanced Monitoring is available for the following database engines:

- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

Enhanced Monitoring is available for all DB instance classes except for the db.m1.small instance class.

Differences between CloudWatch and Enhanced Monitoring metrics

A *hypervisor* creates and runs virtual machines (VMs). Using a hypervisor, an instance can support multiple guest VMs by virtually sharing memory and CPU. CloudWatch gathers metrics about CPU

utilization from the hypervisor for a DB instance. In contrast, Enhanced Monitoring gathers its metrics from an agent on the DB instance.

You might find differences between the CloudWatch and Enhanced Monitoring measurements, because the hypervisor layer performs a small amount of work. The differences can be greater if your DB instances use smaller instance classes. In this scenario, more virtual machines (VMs) are probably managed by the hypervisor layer on a single physical instance.

For descriptions of the Enhanced Monitoring metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#). For more information about CloudWatch metrics, see the [Amazon CloudWatch User Guide](#).

Retention of Enhanced Monitoring metrics

By default, Enhanced Monitoring metrics are stored for 30 days in the CloudWatch Logs. This retention period is different from typical CloudWatch metrics.

To modify the amount of time the metrics are stored in the CloudWatch Logs, change the retention for the RDSOSMetrics log group in the CloudWatch console. For more information, see [Change log data retention in CloudWatch logs](#) in the *Amazon CloudWatch Logs User Guide*.

Cost of Enhanced Monitoring

Enhanced Monitoring metrics are stored in the CloudWatch Logs instead of in CloudWatch metrics. The cost of Enhanced Monitoring depends on the following factors:

- You are charged for Enhanced Monitoring only if you exceed the free tier provided by Amazon CloudWatch Logs. Charges are based on CloudWatch Logs data transfer and storage rates.
- The amount of information transferred for an RDS instance is directly proportional to the defined granularity for the Enhanced Monitoring feature. A smaller monitoring interval results in more frequent reporting of OS metrics and increases your monitoring cost. To manage costs, set different granularities for different instances in your accounts.
- Usage costs for Enhanced Monitoring are applied for each DB instance that Enhanced Monitoring is enabled for. Monitoring a large number of DB instances is more expensive than monitoring only a few.
- DB instances that support a more compute-intensive workload have more OS process activity to report and higher costs for Enhanced Monitoring.

For more information about pricing, see [Amazon CloudWatch pricing](#).

Setting up and enabling Enhanced Monitoring

To use Enhanced Monitoring, you must create an IAM role, and then enable Enhanced Monitoring.

Topics

- [Creating an IAM role for Enhanced Monitoring \(p. 601\)](#)
- [Turning Enhanced Monitoring on and off \(p. 602\)](#)
- [Protecting against the confused deputy problem \(p. 604\)](#)

Creating an IAM role for Enhanced Monitoring

Enhanced Monitoring requires permission to act on your behalf to send OS metric information to CloudWatch Logs. You grant Enhanced Monitoring permissions using an AWS Identity and Access Management (IAM) role. You can either create this role when you enable Enhanced Monitoring or create it beforehand.

Topics

- [Creating the IAM role when you enable Enhanced Monitoring \(p. 602\)](#)
- [Creating the IAM role before you enable Enhanced Monitoring \(p. 602\)](#)

Creating the IAM role when you enable Enhanced Monitoring

When you enable Enhanced Monitoring in the RDS console, Amazon RDS can create the required IAM role for you. The role is named `rds-monitoring-role`. RDS uses this role for the specified DB instance, read replica, or Multi-AZ DB cluster.

To create the IAM role when enabling Enhanced Monitoring

1. Follow the steps in [Turning Enhanced Monitoring on and off \(p. 602\)](#).
2. Set **Monitoring Role** to **Default** in the step where you choose a role.

Creating the IAM role before you enable Enhanced Monitoring

You can create the required role before you enable Enhanced Monitoring. When you enable Enhanced Monitoring, specify your new role's name. You must create this required role if you enable Enhanced Monitoring using the AWS CLI or the RDS API.

The user that enables Enhanced Monitoring must be granted the `PassRole` permission. For more information, see Example 2 in [Granting a user permissions to pass a role to an AWS service](#) in the *IAM User Guide*.

To create an IAM role for Amazon RDS enhanced monitoring

1. Open the [IAM console](#) at <https://console.aws.amazon.com>.
2. In the navigation pane, choose **Roles**.
3. Choose **Create role**.
4. Choose the **AWS service** tab, and then choose **RDS** from the list of services.
5. Choose **RDS - Enhanced Monitoring**, and then choose **Next**.
6. Ensure that the **Permissions policies** shows **AmazonRDSEnhancedMonitoringRole**, and then choose **Next**.
7. For **Role name**, enter a name for your role. For example, enter `emaccess`.

The trusted entity for your role is the AWS service `monitoring.rds.amazonaws.com`.

8. Choose **Create role**.

Turning Enhanced Monitoring on and off

You can turn Enhanced Monitoring on and off using the AWS Management Console, AWS CLI, or RDS API. You choose the RDS DB instances on which you want to turn on Enhanced Monitoring. You can set different granularities for metric collection on each DB instance.

Console

You can turn on Enhanced Monitoring when you create a DB instance, Multi-AZ DB cluster, or read replica, or when you modify a DB instance or Multi-AZ DB cluster. If you modify a DB instance to turn on Enhanced Monitoring, you don't need to reboot your DB instance for the change to take effect.

You can turn on Enhanced Monitoring in the RDS console when you do one of the following actions in the **Databases** page:

- **Create a DB instance or Multi-AZ DB cluster** – Choose **Create database**.
- **Create a read replica** – Choose **Actions**, then **Create read replica**.
- **Modify a DB instance or Multi-AZ DB cluster** – Choose **Modify**.

To turn Enhanced Monitoring on or off in the RDS console

1. Scroll to **Additional configuration**.
2. In **Monitoring**, choose **Enable Enhanced Monitoring** for your DB instance or read replica. To turn Enhanced Monitoring off, choose **Disable Enhanced Monitoring**.
3. Set the **Monitoring Role** property to the IAM role that you created to permit Amazon RDS to communicate with Amazon CloudWatch Logs for you, or choose **Default** to have RDS create a role for you named `rds-monitoring-role`.
4. Set the **Granularity** property to the interval, in seconds, between points when metrics are collected for your DB instance or read replica. The **Granularity** property can be set to one of the following values: 1, 5, 10, 15, 30, or 60.

The fastest that the RDS console refreshes is every 5 seconds. If you set the granularity to 1 second in the RDS console, you still see updated metrics only every 5 seconds. You can retrieve 1-second metric updates by using CloudWatch Logs.

AWS CLI

To turn on Enhanced Monitoring using the AWS CLI, in the following commands, set the `--monitoring-interval` option to a value other than 0 and set the `--monitoring-role-arn` option to the role you created in [Creating an IAM role for Enhanced Monitoring \(p. 601\)](#).

- [create-db-instance](#)
- [create-db-instance-read-replica](#)
- [modify-db-instance](#)
- [create-db-cluster](#) (Multi-AZ DB cluster)
- [modify-db-cluster](#) (Multi-AZ DB cluster)

The `--monitoring-interval` option specifies the interval, in seconds, between points when Enhanced Monitoring metrics are collected. Valid values for the option are 0, 1, 5, 10, 15, 30, and 60.

To turn off Enhanced Monitoring using the AWS CLI, set the `--monitoring-interval` option to 0 in these commands.

Example

The following example turns on Enhanced Monitoring for a DB instance:

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --monitoring-interval 30 \
  --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

For Windows:

```
aws rds modify-db-instance ^
```

```
--db-instance-identifier mydbinstance ^
--monitoring-interval 30 ^
--monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Example

The following example turns on Enhanced Monitoring for a Multi-AZ DB cluster:

For Linux, macOS, or Unix:

```
aws rds modify-db-cluster \
--db-cluster-identifier mydbcluster \
--monitoring-interval 30 \
--monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

For Windows:

```
aws rds modify-db-cluster ^
--db-cluster-identifier mydbcluster ^
--monitoring-interval 30 ^
--monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

RDS API

To turn on Enhanced Monitoring using the RDS API, set the `MonitoringInterval` parameter to a value other than `0` and set the `MonitoringRoleArn` parameter to the role you created in [Creating an IAM role for Enhanced Monitoring \(p. 601\)](#). Set these parameters in the following actions:

- [CreateDBInstance](#)
- [CreateDBInstanceReadReplica](#)
- [ModifyDBInstance](#)
- [CreateDBCluster \(Multi-AZ DB cluster\)](#)
- [ModifyDBCluster \(Multi-AZ DB cluster\)](#)

The `MonitoringInterval` parameter specifies the interval, in seconds, between points when Enhanced Monitoring metrics are collected. Valid values are `0`, `1`, `5`, `10`, `15`, `30`, and `60`.

To turn off Enhanced Monitoring using the RDS API, set `MonitoringInterval` to `0`.

Protecting against the confused deputy problem

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account. For more information, see [The confused deputy problem](#).

To limit the permissions to the resource that Amazon RDS can give another service, we recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in a trust policy for your Enhanced Monitoring role. If you use both global condition context keys, they must use the same account ID.

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. For Amazon RDS, set `aws:SourceArn` to `arn:aws:rds:Region:my-account-id:db:dbname`.

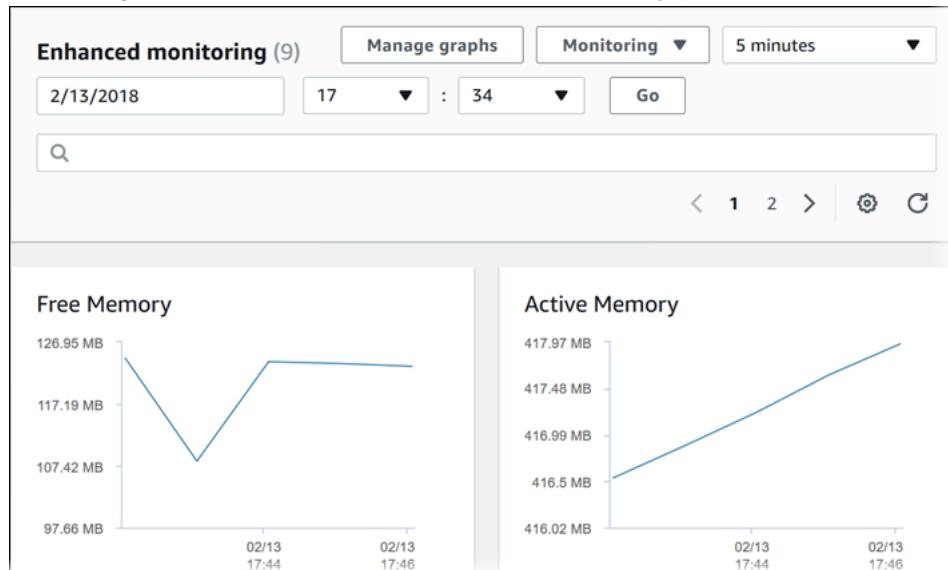
The following example uses the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in a trust policy to prevent the confused deputy problem.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "rds.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole",  
            "Condition": {  
                "StringLike": {  
                    "aws:SourceArn": "arn:aws:rds:Region:my-account-id:db:dbname"  
                },  
                "StringEquals": {  
                    "aws:SourceAccount": "my-account-id"  
                }  
            }  
        }  
    ]  
}
```

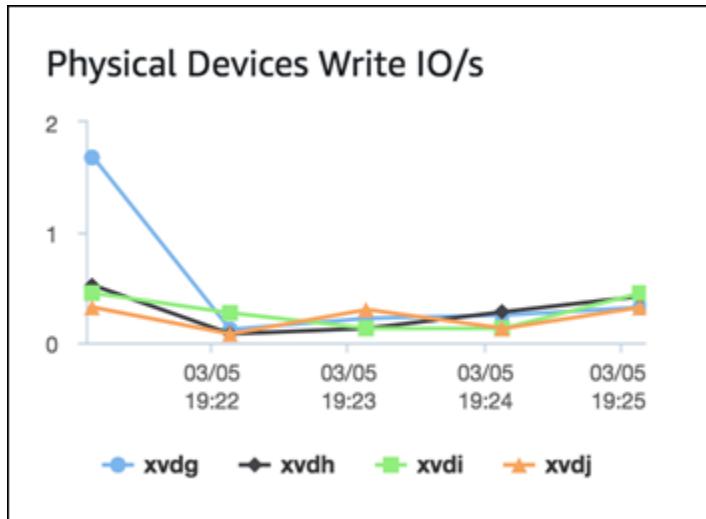
Viewing OS metrics in the RDS console

You can view OS metrics reported by Enhanced Monitoring in the RDS console by choosing **Enhanced monitoring for Monitoring**.

The following example shows the Enhanced Monitoring page. For descriptions of the Enhanced Monitoring metrics, see [OS metrics in Enhanced Monitoring \(p. 633\)](#).



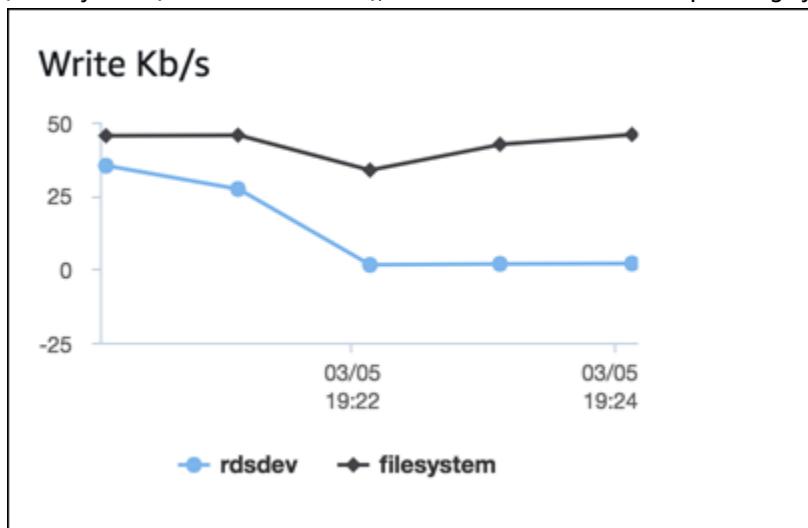
Some DB instances use more than one disk for the DB instance's data storage volume. On those DB instances, the **Physical Devices** graphs show metrics for each one of the disks. For example, the following graph shows metrics for four disks.



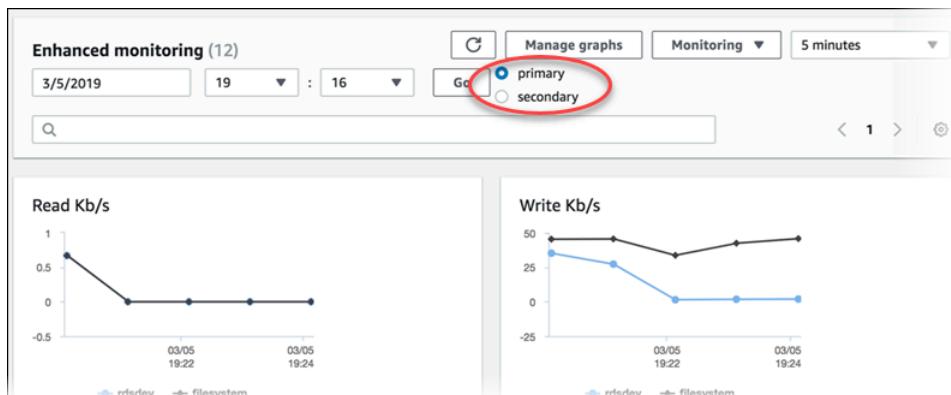
Note

Currently, **Physical Devices** graphs are not available for Microsoft SQL Server DB instances.

When you are viewing aggregated **Disk I/O** and **File system** graphs, the **rdsdev** device relates to the **/rdsdbdata** file system, where all database files and logs are stored. The **filesystem** device relates to the **/** file system (also known as root), where files related to the operating system are stored.



If the DB instance is a Multi-AZ deployment, you can view the OS metrics for the primary DB instance and its Multi-AZ standby replica. In the **Enhanced monitoring** view, choose **primary** to view the OS metrics for the primary DB instance, or choose **secondary** to view the OS metrics for the standby replica.



For more information about Multi-AZ deployments, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Note

Currently, viewing OS metrics for a Multi-AZ standby replica is not supported for MariaDB or Microsoft SQL Server DB instances.

If you want to see details for the processes running on your DB instance, choose **OS process list** for **Monitoring**.

The **Process List** view is shown following.

Process List						
<input type="text"/> Filter process list						
NAME	VIRT	RES	CPU%	MEM%	VMLIMIT	
postgres [3181] ^t	283.55 MB	17.11 MB	0.02	1.72		
postgres: rdsadmin rdsadmin localhost(40156) idle [2953] ^t	384.7 MB	9.51 MB	0.02	0.95		

The Enhanced Monitoring metrics shown in the **Process list** view are organized as follows:

- **RDS child processes** – Shows a summary of the RDS processes that support the DB instance, for example mysqld for MySQL DB instances. Process threads appear nested beneath the parent process. Process threads show CPU utilization only as other metrics are the same for all threads for the process. The console displays a maximum of 100 processes and threads. The results are a combination of the top CPU consuming and memory consuming processes and threads. If there are more than 50 processes and more than 50 threads, the console displays the top 50 consumers in each category. This display helps you identify which processes are having the greatest impact on performance.
- **RDS processes** – Shows a summary of the resources used by the RDS management agent, diagnostics monitoring processes, and other AWS processes that are required to support RDS DB instances.
- **OS processes** – Shows a summary of the kernel and system processes, which generally have minimal impact on performance.

The items listed for each process are:

- **VIRT** – Displays the virtual size of the process.
- **RES** – Displays the actual physical memory being used by the process.
- **CPU%** – Displays the percentage of the total CPU bandwidth being used by the process.
- **MEM%** – Displays the percentage of the total memory being used by the process.

The monitoring data that is shown in the RDS console is retrieved from Amazon CloudWatch Logs. You can also retrieve the metrics for a DB instance as a log stream from CloudWatch Logs. For more information, see [Viewing OS metrics using CloudWatch Logs \(p. 608\)](#).

Enhanced Monitoring metrics are not returned during the following:

- A failover of the DB instance.
- Changing the instance class of the DB instance (scale compute).

Enhanced Monitoring metrics are returned during a reboot of a DB instance because only the database engine is rebooted. Metrics for the operating system are still reported.

Viewing OS metrics using CloudWatch Logs

After you have enabled Enhanced Monitoring for your DB instance or Multi-AZ DB cluster, you can view the metrics for it using CloudWatch Logs, with each log stream representing a single DB instance or DB cluster being monitored. The log stream identifier is the resource identifier (`DbiResourceId`) for the DB instance or DB cluster.

To view Enhanced Monitoring log data

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. If necessary, choose the AWS Region that your DB instance or Multi-AZ DB cluster is in. For more information, see [Regions and endpoints](#) in the *Amazon Web Services General Reference*.
3. Choose **Logs** in the navigation pane.
4. Choose **RDSOSMetrics** from the list of log groups.

In a Multi-AZ DB instance deployment, log files with `-secondary` appended to the name are for the Multi-AZ standby replica.

The screenshot shows the CloudWatch Log Groups interface. At the top, there are buttons for 'Search Log Group', 'Create Log Stream', and 'Delete Log Stream'. Below that is a 'Filter' input field set to 'Log Stream Name Prefix'. The main area displays a table of log streams. The first row has a checkbox and the text 'Log Streams'. The second row contains two entries: 'db-SORJBHOPBSMWGRI5EJW3KMYOTU-secondary' and 'db-SORJBHOPBSMWGRI5EJW3KMYOTU'. A red box highlights the secondary log stream. To the right of the streams, there is a column for 'Last Event Time' with values '2019-03-05 12:12 UTC-8' and '2019-03-05 12:07 UTC-8' respectively. Navigation arrows and a refresh icon are at the top right of the table area.

Log Streams	Last Event Time
db-SORJBHOPBSMWGRI5EJW3KMYOTU-secondary	2019-03-05 12:12 UTC-8
db-SORJBHOPBSMWGRI5EJW3KMYOTU	2019-03-05 12:07 UTC-8

5. Choose the log stream that you want to view from the list of log streams.

Metrics reference for Amazon RDS

In this reference, you can find descriptions of Amazon RDS metrics for Amazon CloudWatch, Performance Insights, and Enhanced Monitoring.

Topics

- [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#)
- [Amazon CloudWatch dimensions for Amazon RDS \(p. 616\)](#)
- [Amazon CloudWatch metrics for Performance Insights \(p. 617\)](#)
- [Performance Insights counter metrics \(p. 618\)](#)
- [SQL statistics for Performance Insights \(p. 628\)](#)
- [OS metrics in Enhanced Monitoring \(p. 633\)](#)

Amazon CloudWatch metrics for Amazon RDS

Amazon RDS publishes metrics to Amazon CloudWatch in the AWS/RDS and AWS/Usage namespaces.

Topics

- [Amazon CloudWatch instance-level metrics for Amazon RDS \(p. 609\)](#)
- [Amazon CloudWatch usage metrics for Amazon RDS \(p. 615\)](#)

Amazon CloudWatch instance-level metrics for Amazon RDS

The AWS/RDS namespace in Amazon CloudWatch includes the following instance-level metrics.

Note

The Amazon RDS console might display metrics in units that are different from the units sent to Amazon CloudWatch. For example, the Amazon RDS console might display a metric in megabytes (MB), while the metric is sent to Amazon CloudWatch in bytes.

Metric	Console name	Description	Units
BinLogDiskUsage	Binary Log Disk Usage (MB)	The amount of disk space occupied by binary logs. If automatic backups are enabled for MySQL and MariaDB instances, including read replicas, binary logs are created.	Bytes
BurstBalance	Burst Balance (Percent)	The percent of General Purpose SSD (gp2) burst-bucket I/O credits available.	Percent
CheckpointLag	Checkpoint Lag (Milliseconds)	The amount of time since the most recent checkpoint. Applies to only RDS for PostgreSQL.	Seconds
ConnectionAttempts	Connection Attempts (Count)	The number of attempts to connect to an instance, whether successful or not.	Count
CPUUtilization	CPU Utilization (Percent)	The percentage of CPU utilization.	Percent
CPUTCreditUsage	CPU Credit Usage (Count)	(T2 instances) The number of CPU credits spent by the instance for CPU utilization.	Credits (vCPU-minutes)

Metric	Console name	Description	Units
		<p>One CPU credit equals one vCPU running at 100 percent utilization for one minute or an equivalent combination of vCPUs, utilization, and time. For example, you might have one vCPU running at 50 percent utilization for two minutes or two vCPUs running at 25 percent utilization for two minutes.</p> <p>CPU credit metrics are available at a five-minute frequency only. If you specify a period greater than five minutes, use the Sum statistic instead of the Average statistic.</p>	
CPUCreditBalance	CPU Credit Balance (Count)	<p>(T2 instances) The number of earned CPU credits that an instance has accrued since it was launched or started. For T2 Standard, the CPUCreditBalance also includes the number of launch credits that have been accrued.</p> <p>Credits are accrued in the credit balance after they are earned, and removed from the credit balance when they are spent. The credit balance has a maximum limit, determined by the instance size. After the limit is reached, any new credits that are earned are discarded. For T2 Standard, launch credits don't count towards the limit.</p> <p>The credits in the CPUCreditBalance are available for the instance to spend to burst beyond its baseline CPU utilization.</p> <p>When an instance is running, credits in the CPUCreditBalance don't expire. When the instance stops, the CPUCreditBalance does not persist, and all accrued credits are lost.</p> <p>CPU credit metrics are available at a five-minute frequency only.</p> <p>Launch credits work the same way in Amazon RDS as they do in Amazon EC2. For more information, see Launch credits in the <i>Amazon Elastic Compute Cloud User Guide for Linux Instances</i>.</p>	Credits (vCPU-minutes)

Metric	Console name	Description	Units
DatabaseConnections	DB Connections (Count)	<p>The number of client network connections to the database instance.</p> <p>The number of database sessions can be higher than the metric value because the metric value doesn't include the following:</p> <ul style="list-style-type: none"> • Sessions that no longer have a network connection but which the database hasn't cleaned up • Sessions created by the database engine for its own purposes • Sessions created by the database engine's parallel execution capabilities • Sessions created by the database engine job scheduler • Amazon RDS connections 	Count
DiskQueueDepth	Queue Depth (Count)	The number of outstanding I/Os (read/write requests) waiting to access the disk.	Count
EBSByteBalance %	EBS Byte Balance (Percent)	<p>The percentage of throughput credits remaining in the burst bucket of your RDS database. This metric is available for basic monitoring only.</p> <p>The metric value is based on the throughput and IOPS of all volumes, including the root volume, rather than on only those volumes containing database files.</p> <p>To find the instance sizes that support this metric, see the instance sizes with an asterisk (*) in the EBS optimized by default table in <i>Amazon EC2 User Guide for Linux Instances</i>. The Sum statistic is not applicable to this metric.</p>	Percent

Metric	Console name	Description	Units
EBSIOBalance%	EBS IO Balance (Percent)	<p>The percentage of I/O credits remaining in the burst bucket of your RDS database. This metric is available for basic monitoring only.</p> <p>The metric value is based on the throughput and IOPS of all volumes, including the root volume, rather than on only those volumes containing database files.</p> <p>To find the instance sizes that support this metric, see the instance sizes with an asterisk (*) in the EBS optimized by default table in <i>Amazon EC2 User Guide for Linux Instances</i>. The Sum statistic is not applicable to this metric.</p> <p>This metric is different from BurstBalance. To learn how to use this metric, see Improving application performance and reducing costs with Amazon EBS-Optimized Instance burst capability.</p>	Percent
FailedSQLServerJobs	Failed SQL Server Agent Jobs Count (Count/Minute)	The number of failed Microsoft SQL Server Agent jobs during the last minute.	Count/Minute
FreeableMemory	Freeable Memory (MB)	<p>The amount of available random access memory.</p> <p>For MariaDB, MySQL, Oracle, and PostgreSQL DB instances, this metric reports the value of the MemAvailable field of /proc/meminfo.</p>	Bytes
FreeLocalStorage	Free Local Storage (MB)	<p>The amount of available local storage space.</p> <p>This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes. The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.</p> <p>(This doesn't apply to Aurora Serverless v2.)</p>	Bytes

Metric	Console name	Description	Units
FreeStorageSpace	Free Storage Space (MB)	The amount of available storage space.	Bytes
MaximumUsedTransactionIDs	Maximum Used Transaction IDs (Count)	The maximum transaction IDs that have been used. Applies to only PostgreSQL.	Count
NetworkReceiveThroughput	Network Receive Throughput (MB/Second)	The incoming (receive) network traffic on the DB instance, including both customer database traffic and Amazon RDS traffic used for monitoring and replication.	Bytes/Second
NetworkTransmitThroughput	Network Transmit Throughput (MB/Second)	The outgoing (transmit) network traffic on the DB instance, including both customer database traffic and Amazon RDS traffic used for monitoring and replication.	Bytes/Second
OldestReplicationLag	Oldest Replication Lag (MB)	The lagging size of the replica lagging the most in terms of write-ahead log (WAL) data received. Applies to PostgreSQL.	Bytes
ReadIOPS	Read IOPS (Count/Second)	The average number of disk read I/O operations per second.	Count/Second
ReadIOPSLocalStorage	Read IOPS Local Storage (Count/Second)	<p>The average number of disk read I/O operations to local storage per second.</p> <p>This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes. The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.</p>	Count/Second
ReadLatency	Read Latency (Milliseconds)	The average amount of time taken per disk I/O operation.	Seconds
ReadLatencyLocalStorage	Read Latency Local Storage (Milliseconds)	<p>The average amount of time taken per disk I/O operation for local storage.</p> <p>This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes. The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.</p>	Seconds
ReadThroughput	Read Throughput (MB/Second)	The average number of bytes read from disk per second.	Bytes/Second

Metric	Console name	Description	Units
ReadThroughputLocalStorage	Read Throughput Local Storage (MB/Second)	The average number of bytes read from disk per second for local storage. This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes . The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.	Bytes/Second
ReplicaLag	Replica Lag (Milliseconds)	For read replica configurations, the amount of time a read replica DB instance lags behind the source DB instance. Applies to MariaDB, Microsoft SQL Server, MySQL, Oracle, and PostgreSQL read replicas. For Multi-AZ DB clusters, the difference in time between the latest transaction on the writer DB instance and the latest applied transaction on a reader DB instance.	Seconds
ReplicationSlotDiskUsage	Replica Slot Disk Usage (MB)	The disk space used by replication slot files. Applies to PostgreSQL.	Bytes
SwapUsage	Swap Usage (MB)	The amount of swap space used on the DB instance. This metric is not available for SQL Server.	Bytes
TransactionLogsDiskUsage	Transaction Logs Disk Usage (MB)	The disk space used by transaction logs. Applies to PostgreSQL.	Bytes
TransactionLogsGeneration	TransactionLogs Generation (MB/Second)	The size of transaction logs generated per second. Applies to PostgreSQL.	Bytes/Second
WriteIOPS	Write IOPS (Count/Second)	The average number of disk write I/O operations per second.	Count/Second

Metric	Console name	Description	Units
WriteIOPSLocalStorage	Write IOPS Local Storage (Count/Second)	The average number of disk write I/O operations per second on local storage. This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes . The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.	Count/Second
WriteLatency	Write Latency (Milliseconds)	The average amount of time taken per disk I/O operation.	Seconds
WriteLatencyLocalStorage	Write Latency Local Storage (Milliseconds)	The average amount of time taken per disk I/O operation on local storage. This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes . The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.	Milliseconds
WriteThroughput	Write Throughput (MB/Second)	The average number of bytes written to disk per second.	Bytes/Second
WriteThroughputLocalStorage	Write Storage Throughput Local Storage (MB/Second)	The average number of bytes written to disk per second for local storage. This metric only applies to DB instance classes with NVMe SSD instance store volumes. For information about Amazon EC2 instances with NVMe SSD instance store volumes, see Instance store volumes . The equivalent RDS DB instance classes have the same instance store volumes. For example, the db.m6gd and db.r6gd DB instance classes have NVMe SSD instance store volumes.	Bytes/Second

Amazon CloudWatch usage metrics for Amazon RDS

The AWS/Usage namespace in Amazon CloudWatch includes account-level usage metrics for your Amazon RDS service quotas. CloudWatch collects usage metrics automatically for all AWS Regions.

For more information, see [CloudWatch usage metrics](#) in the *Amazon CloudWatch User Guide*. For more information about quotas, see [Quotas and constraints for Amazon RDS \(p. 2135\)](#) and [Requesting a quota increase](#) in the *Service Quotas User Guide*.

Metric	Description	Units*
AllocatedStorage	The total storage for all DB instances. The sum excludes temporary migration instances.	Gigabytes
DBClusterParameterGroups	The number of DB cluster parameter groups in your AWS account. The count excludes default parameter groups.	Count
DBClusters	The number of Amazon Aurora DB clusters in your AWS account.	Count
DBInstances	The number of DB instances in your AWS account.	Count
DBParameterGroups	The number of DB parameter groups in your AWS account. The count excludes the default DB parameter groups.	Count
DBSecurityGroups	The number of security groups in your AWS account. The count excludes the default security group and the default VPC security group.	Count
DBSubnetGroups	The number of DB subnet groups in your AWS account. The count excludes the default subnet group.	Count
ManualClusterSnapshots	The number of manually created DB cluster snapshots in your AWS account. The count excludes invalid snapshots.	Count
ManualSnapshots	The number of manually created DB snapshots in your AWS account. The count excludes invalid snapshots.	Count
OptionGroups	The number of option groups in your AWS account. The count excludes the default option groups.	Count
ReservedDBInstances	The number of reserved DB instances in your AWS account. The count excludes retired or declined instances.	Count

* Amazon RDS doesn't publish units for usage metrics to CloudWatch. The units only appear in the documentation.

Amazon CloudWatch dimensions for Amazon RDS

You can filter Amazon RDS metrics data by using any dimension in the following table.

Dimension	Filters the requested data for ...
DBInstanceIdentifier	A specific DB instance.
DatabaseClass	All instances in a database class. For example, you can aggregate metrics for all instances that belong to the database class db.r5.large.
EngineName	The identified engine name only. For example, you can aggregate metrics for all instances that have the engine name postgres.

Dimension	Filters the requested data for ...
SourceRegion	The specified Region only. For example, you can aggregate metrics for all DB instances in the us-east-1 Region.

Amazon CloudWatch metrics for Performance Insights

Performance Insights automatically publishes metrics to Amazon CloudWatch. The same data can be queried from Performance Insights, but having the metrics in CloudWatch makes it easy to add CloudWatch alarms. It also makes it easy to add the metrics to existing CloudWatch Dashboards.

Metric	Description
DBLoad	The number of active sessions for the DB engine. Typically, you want the data for the average number of active sessions. In Performance Insights, this data is queried as db.load.avg.
DBLoadCPU	The number of active sessions where the wait event type is CPU. In Performance Insights, this data is queried as db.load.avg, filtered by the wait event type CPU.
DBLoadNonCPU	The number of active sessions where the wait event type is not CPU.

Note

These metrics are published to CloudWatch only if there is load on the DB instance.

You can examine these metrics using the CloudWatch console, the AWS CLI, or the CloudWatch API.

For example, you can get the statistics for the DBLoad metric by running the [get-metric-statistics](#) command.

```
aws cloudwatch get-metric-statistics \
--region us-west-2 \
--namespace AWS/RDS \
--metric-name DBLoad \
--period 60 \
--statistics Average \
--start-time 1532035185 \
--end-time 1532036185 \
--dimensions Name=DBInstanceIdentifier,Value=db-loadtest-0
```

This example generates output similar to the following.

```
{
  "Datapoints": [
    {
      "Timestamp": "2021-07-19T21:30:00Z",
      "Unit": "None",
      "Average": 2.1
    },
    {
      "Timestamp": "2021-07-19T21:30:00Z",
      "Unit": "None",
      "Average": 2.1
    }
  ]
}
```

```
"Timestamp": "2021-07-19T21:34:00Z",
"Unit": "None",
"Average": 1.7
},
{
"Timestamp": "2021-07-19T21:35:00Z",
"Unit": "None",
"Average": 2.8
},
{
"Timestamp": "2021-07-19T21:31:00Z",
"Unit": "None",
"Average": 1.5
},
{
"Timestamp": "2021-07-19T21:32:00Z",
"Unit": "None",
"Average": 1.8
},
{
"Timestamp": "2021-07-19T21:29:00Z",
"Unit": "None",
"Average": 3.0
},
{
"Timestamp": "2021-07-19T21:33:00Z",
"Unit": "None",
"Average": 2.4
}
],
"Label": "DBLoad"
}
```

For more information about CloudWatch, see [What is Amazon CloudWatch?](#) in the *Amazon CloudWatch User Guide*.

Performance Insights counter metrics

Counter metrics are operating system and database performance metrics in the Performance Insights dashboard. To help identify and analyze performance problems, you can correlate counter metrics with DB load.

Topics

- [Performance Insights counters for Amazon RDS for MariaDB and MySQL \(p. 618\)](#)
- [Performance Insights counters for Amazon RDS for Microsoft SQL Server \(p. 623\)](#)
- [Performance Insights counters for Amazon RDS for Oracle \(p. 624\)](#)
- [Performance Insights counters for Amazon RDS for PostgreSQL \(p. 626\)](#)

Performance Insights counters for Amazon RDS for MariaDB and MySQL

The following database counters are available with Performance Insights for Amazon RDS for MariaDB and MySQL.

Topics

- [Native counters for RDS for MariaDB and RDS for MySQL \(p. 619\)](#)
- [Non-native counters for Amazon RDS for MariaDB and MySQL \(p. 621\)](#)

Native counters for RDS for MariaDB and RDS for MySQL

Native metrics are defined by the database engine and not by Amazon RDS. For definitions of these native metrics, see [Server Status Variables](#) in the MySQL documentation.

Counter	Type	Unit	Metric
Com_analyze	SQL	Queries per second	db.SQL.Com_analyze
Com_optimize	SQL	Queries per second	db.SQL.Com_optimize
Com_select	SQL	Queries per second	db.SQL.Com_select
Connections	SQL	The number of connection attempts per minute (successful or not) to the MySQL server	db.Users.Connections
Innodb_rows_deleted	SQL	Rows per second	db.SQL.Innodb_rows_deleted
Innodb_rows_inserted	SQL	Rows per second	db.SQL.Innodb_rows_inserted
Innodb_rows_read	SQL	Rows per second	db.SQL.Innodb_rows_read
Innodb_rows_updated	SQL	Rows per second	db.SQL.Innodb_rows_updated
Select_full_join	SQL	Queries per second	db.SQL.Select_full_join
Select_full_range_join	SQL	Queries per second	db.SQL.Select_full_range_join
Select_range	SQL	Queries per second	db.SQL.Select_range
Select_range_check	SQL	Queries per second	db.SQL.Select_range_check
Select_scan	SQL	Queries per second	db.SQL.Select_scan
Slow_queries	SQL	Queries per second	db.SQL.Slow_queries
Sort_merge_passes	SQL	Queries per second	db.SQL.Sort_merge_passes
Sort_range	SQL	Queries per second	db.SQL.Sort_range

Counter	Type	Unit	Metric
Sort_rows	SQL	Queries per second	db.SQL.Sort_rows
Sort_scan	SQL	Queries per second	db.SQL.Sort_scan
Questions	SQL	Queries per second	db.SQL.Questions
Innodb_row_lock_time	Locks	Milliseconds (average)	db.Locks.Innodb_row_lock_time
Table_locks_immediate	Locks	Requests per second	db.Locks.Table_locks_immediate
Table_locks_waited	Locks	Requests per second	db.Locks.Table_locks_waited
Aborted_clients	Users	Connections	db.Users.Aborted_clients
Aborted_connects	Users	Connections	db.Users.Aborted_connects
Threads_created	Users	Connections	db.Users.Threads_created
Threads_running	Users	Connections	db.Users.Threads_running
Innodb_data_writes	I/O	Operations per second	db.IO.Innodb_data_writes
Innodb_dblwr_writes	I/O	Operations per second	db.IO.Innodb_dblwr_writes
Innodb_log_write_requests	I/O	Operations per second	db.IO.Innodb_log_write_requests
Innodb_log_writes	I/O	Operations per second	db.IO.Innodb_log_writes
Innodb_pages_written	I/O	Pages per second	db.IO.Innodb_pages_written
Created_tmp_disk_tables	Temp	Tables per second	db.Temp.Created_tmp_disk_tables
Created_tmp_tables	Temp	Tables per second	db.Temp.Created_tmp_tables
Innodb_buffer_pool_pages_data	Cache	Pages	db.Cache.Innodb_buffer_pool_pages_data
Innodb_buffer_pool_pages_total	Cache	Pages	db.Cache.Innodb_buffer_pool_pages_total
Innodb_buffer_pool_read_requests	Cache	Pages per second	db.Cache.Innodb_buffer_pool_read_requests
Innodb_buffer_pool_reads	Cache	Pages per second	db.Cache.Innodb_buffer_pool_reads
Opened_tables	Cache	Tables	db.Cache.Opened_tables

Counter	Type	Unit	Metric
Opened_table_definitions	Cache	Tables	db.Cache.Opened_table_definitions
Qcache_hits	Cache	Queries	db.Cache.Qcache_hits

Non-native counters for Amazon RDS for MariaDB and MySQL

Non-native counter metrics are counters defined by Amazon RDS. A non-native metric can be a metric that you get with a specific query. A non-native metric also can be a derived metric, where two or more native counters are used in calculations for ratios, hit rates, or latencies.

Counter	Type	Metric	Description	Definition
innodb_buffer_pool_hits	Cache	db.Cache.innoDB_buffer_pool_hits	Number of reads that InnoDB could satisfy from the buffer pool.	innodb_buffer_pool_read_requests - innodb_buffer_pool_reads
innodb_buffer_pool_hit_rate	Cache	db.Cache.innoDB_buffer_pool_hit_rate	Percentage of reads that InnoDB could satisfy from the buffer pool.	100 * innodb_buffer_pool_read_requests / (innodb_buffer_pool_read_requests + innodb_buffer_pool_reads)
innodb_buffer_pool_usage	Cache	db.Cache.innoDB_buffer_pool_usage	Percentage of the InnoDB buffer pool that contains data (pages).	Innodb_buffer_pool_pages_data / Innodb_buffer_pool_pages_total * 100.0

Note
When using compressed tables, this value can vary. For more information, see the information about Innodb_buffer_pool_pages_data and Innodb_buffer_pool_pages_total in Server.

Counter	Type	Metric	Description	Definition
			Status Variables in the MySQL documentation.	
query_cache_hit_rate	Cache	db.Cache.query_cache_hit	MySQL result set cache (query cache) hit ratio.	Qcache_hits / (QCache_hits + Com_select) * 100
innodb_datafile_writes_to_d	IO	db.IO.innoDB_datafile_writes	The number of InnoDB data file writes to disk, excluding double write and redo logging write operations.	Innodb_data_writes - Innodb_log_writes - Innodb dblwr_writes
innodb_rows_changed	SQL	db.SQL.innodb_rows_change	The total InnoDB row operations.	db.SQL.Innodb_rows_inserted + db.SQL.Innodb_rows_deleted + db.SQL.Innodb_rows_updated
active_transactions	Transactions	db.Transactions.active_transactions	The total active transactions.	SELECT COUNT(1) AS active_transactions FROM INFORMATION_SCHEMA.INNODB_TRX
trx_rseg_history_len	Transactions	db.Transactions.trx_rseg_history	History of the undo log pages for committed transactions that is maintained by the InnoDB transaction system to implement multi-version concurrency control. For more information about undo log records details, see https://dev.mysql.com/doc/refman/8.0/en/innodb-multi-versioning.html in the MySQL documentation.	SELECT COUNT AS trx_rseg_history_len FROM INFORMATION_SCHEMA.INNODB_METRIC WHERE NAME='trx_rseg_history_len'

Counter	Type	Metric	Description	Definition
innodb_deadlocks	Locks	db.Locks.innodb_deadlocks	The total number of deadlocks.	SELECT COUNT AS innodb_deadlocks FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_deadlocks'
innodb_lock_timeouts	Locks	db.Locks.innodb_lock_timeouts	The total number of locks that timed out.	SELECT COUNT AS innodb_lock_timeouts FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_timeouts'
innodb_row_lock_waits	Locks	db.Locks.innodb_row_lock_waits	The total number of row locks that resulted in a wait.	SELECT COUNT AS innodb_row_lock_waits FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_row_lock_waits'

Performance Insights counters for Amazon RDS for Microsoft SQL Server

The following database counters are available with Performance Insights for RDS for Microsoft SQL Server.

Native counters for RDS for Microsoft SQL Server

Native metrics are defined by the database engine and not by Amazon RDS. You can find definitions for these native metrics in [Use SQL Server Objects](#) in the Microsoft SQL Server documentation.

Counter	Type	Unit	Metric
Forwarded Records	Access Methods	Records per second	db.Access Methods.Forwarded Records
Page Splits	Access Methods	Splits per second	db.Access Methods.Page Splits
Buffer cache hit ratio	Buffer Manager	Ratio	db.Buffer Manager.Buffer cache hit ratio
Page life expectancy	Buffer Manager	Expectancy in seconds	db.Buffer Manager.Page life expectancy
Page lookups	Buffer Manager	Lookups per second	db.Buffer Manager.Page lookups
Page reads	Buffer Manager	Reads per second	db.Buffer Manager.Page reads

Counter	Type	Unit	Metric
Page writes	Buffer Manager	Writes per second	db.Buffer Manager.Page writes
Active Transactions	Databases	Transactions	db.Databases.Active Transactions (_Total)
Log Bytes Flushed	Databases	Bytes flushed per second	db.Databases.Log Bytes Flushed (_Total)
Log Flush Waits	Databases	Waits per second	db.Databases.Log Flush Waits (_Total)
Log Flushes	Databases	Flushes per second	db.Databases.Log Flushes (_Total)
Write Transactions	Databases	Transactions per second	db.Databases.Write Transactions (_Total)
Processes blocked	General Statistics	Processes blocked	db.General Statistics.Processes blocked
User Connections	General Statistics	Connections	db.General Statistics.User Connections
Latch Waits	Latches	Waits per second	db.Latches.Latch Waits
Number of Deadlocks	Locks	Deadlocks per second	db.Locks.Number of Deadlocks (_Total)
Memory Grants Pending	Memory Manager	Memory grants	db.Memory Manager.Memory Grants Pending
Batch Requests	SQL Statistics	Requests per second	db.SQL Statistics.Batch Requests
SQL Compilations	SQL Statistics	Compilations per second	db.SQL Statistics.SQL Compilations
SQL Re-Compilations	SQL Statistics	Re-compilations per second	db.SQL Statistics.SQL Re-Compilations

Performance Insights counters for Amazon RDS for Oracle

The following database counters are available with Performance Insights for RDS for Oracle.

Native counters for RDS for Oracle

Native metrics are defined by the database engine and not by Amazon RDS. You can find definitions for these native metrics in [Statistics Descriptions](#) in the Oracle documentation.

Note

For the CPU used by this session counter metric, the unit has been transformed from the native centiseconds to active sessions to make the value easier to use. For example, CPU send in the DB Load chart represents the demand for CPU. The counter metric CPU used by this

session represents the amount of CPU used by Oracle sessions. You can compare CPU send to the CPU used by this session counter metric. When demand for CPU is higher than CPU used, sessions are waiting for CPU time.

Counter	Type	Unit	Metric
CPU used by this session	User	Active sessions	db.User.CPU used by this session
SQL*Net roundtrips to/from client	User	Roundtrips per second	db.User.SQL*Net roundtrips to/from client
Bytes received via SQL*Net from client	User	Bytes per second	db.User.bytes received via SQL*Net from client
User commits	User	Commits per second	db.User.user commits
Logons cumulative	User	Logons per second	db.User.logons cumulative
User calls	User	Calls per second	db.User.user calls
Bytes sent via SQL*Net to client	User	Bytes per second	db.User.bytes sent via SQL*Net to client
User rollbacks	User	Rollbacks per second	db.User.user rollbacks
Redo size	Redo	Bytes per second	db.Redo.redo size
Parse count (total)	SQL	Parses per second	db.SQL.parse count (total)
Parse count (hard)	SQL	Parses per second	db.SQL.parse count (hard)
Table scan rows gotten	SQL	Rows per second	db.SQL.table scan rows gotten
Sorts (memory)	SQL	Sorts per second	db.SQL.sorts (memory)
Sorts (disk)	SQL	Sorts per second	db.SQL.sorts (disk)
Sorts (rows)	SQL	Sorts per second	db.SQL.sorts (rows)
Physical read bytes	Cache	Bytes per second	db.Cache.physical read bytes
DB block gets	Cache	Blocks per second	db.Cache.db block gets
DBWR checkpoints	Cache	Checkpoints per minute	db.Cache.DBWR checkpoints
Physical reads	Cache	Reads per second	db.Cache.physical reads
Consistent gets from cache	Cache	Gets per second	db.Cache.consistent gets from cache
DB block gets from cache	Cache	Gets per second	db.Cache.db block gets from cache

Counter	Type	Unit	Metric
Consistent gets	Cache	Gets per second	db.Cache.consistent_gets

Performance Insights counters for Amazon RDS for PostgreSQL

The following database counters are available with Performance Insights for Amazon RDS for PostgreSQL.

Topics

- [Native counters for Amazon RDS for PostgreSQL \(p. 626\)](#)
- [Non-native counters for Amazon RDS for PostgreSQL \(p. 627\)](#)

Native counters for Amazon RDS for PostgreSQL

Native metrics are defined by the database engine and not by Amazon RDS. You can find definitions for these native metrics in [Viewing Statistics](#) in the PostgreSQL documentation.

Counter	Type	Unit	Metric
blk_hit	Cache	Blocks per second	db.Cache.blk_hit
buffers_alloc	Cache	Blocks per second	db.Cache.buffers_alloc
buffers_checkpoint	Checkpoint	Blocks per second	db.Checkpoint.buffers_checkpoint
checkpoint_sync_time	Checkpoint	Milliseconds per checkpoint	db.Checkpoint.checkpoint_sync_time
checkpoint_write_time	Checkpoint	Milliseconds per checkpoint	db.Checkpoint.checkpoint_write_time
checkpoints_req	Checkpoint	Checkpoints per minute	db.Checkpoint.checkpoints_req
checkpoints_timed	Checkpoint	Checkpoints per minute	db.Checkpoint.checkpoints_timed
maxwritten_clean	Checkpoint	Bgwriter clean stops per minute	db.Checkpoint.maxwritten_clean
deadlocks	Concurrency	Deadlocks per minute	db.Concurrency.deadlocks
blk_read_time	I/O	Milliseconds	db.IO.blk_read_time
blks_read	I/O	Blocks per second	db.IO.blks_read
buffers_backend	I/O	Blocks per second	db.IO.buffers_backend
buffers_backend_fsync	I/O	Blocks per second	db.IO.buffers_backend_fsync
buffers_clean	I/O	Blocks per second	db.IO.buffers_clean
tup_deleted	SQL	Tuples per second	db.SQL.tup_deleted
tup_fetched	SQL	Tuples per second	db.SQL.tup_fetched

Counter	Type	Unit	Metric
tup_inserted	SQL	Tuples per second	db.SQL.tup_inserted
tup_returned	SQL	Tuples per second	db.SQL.tup_returned
tup_updated	SQL	Tuples per second	db.SQL.tup_updated
temp_bytes	Temp	Bytes per second	db.Temp.temp_bytes
temp_files	Temp	Files per minute	db.Temp.temp_files
active_transactions	Transactions	Transactions	db.Transactions.active_transactions
blocked_transactions	Transactions	Transactions	db.Transactions.blocked_transactions
max_used_xact_ids	Transactions	Transactions	db.Transactions.max_used_xact_ids
xact_commit	Transactions	Commits per second	db.Transactions.xact_commit
xact_rollback	Transactions	Rollbacks per second	db.Transactions.xact_rollback
numbackends	User	Connections	db.User.numbackends
archived_count	Write-ahead log (WAL)	Files per minute	db.WAL.archived_count
archive_failed_count	WAL	Files per minute	db.WAL.archive_failed_count

Non-native counters for Amazon RDS for PostgreSQL

Non-native counter metrics are counters defined by Amazon RDS. A non-native metric can be a metric that you get with a specific query. A non-native metric also can be a derived metric, where two or more native counters are used in calculations for ratios, hit rates, or latencies.

Counter	Type	Metric	Description	Definition
checkpoint_sync_lateness	Checkpoint	db.Checkpoint.checkpoint_sync_lateness	The total amount of time that has been spent in the portion of checkpoint processing where files are synchronized to disk.	checkpoint_sync_time / (checkpoints_timed + checkpoints_req)
checkpoint_write_lateness	Checkpoint	db.Checkpoint.checkpoint_write_lateness	The total amount of time that has been spent in the portion of checkpoint processing where files are written to disk.	checkpoint_write_time / (checkpoints_timed + checkpoints_req)
read_latency	I/O	db.IO.read_latency	The time spent reading data file blocks by backends in this instance.	blk_read_time / blks_read

SQL statistics for Performance Insights

SQL statistics are performance-related metrics about SQL queries that are collected by Performance Insights. Performance Insights gathers statistics for each second that a query is running and for each SQL call.

A SQL digest is a composite of all queries having a given pattern but not necessarily having the same literal values. The digest replaces literal values with a question mark. For example, `SELECT * FROM emp WHERE lname= ?`. This digest might consist of the following child queries:

```
SELECT * FROM emp WHERE lname = 'Sanchez'  
SELECT * FROM emp WHERE lname = 'Olagappan'  
SELECT * FROM emp WHERE lname = 'Wu'
```

All engines support SQL statistics for digest queries.

Topics

- [SQL statistics for MariaDB and MySQL \(p. 628\)](#)
- [SQL statistics for Oracle \(p. 630\)](#)
- [SQL statistics for RDS PostgreSQL \(p. 632\)](#)

SQL statistics for MariaDB and MySQL

MariaDB and MySQL collect SQL statistics only at the digest level. No statistics are shown at the statement level.

Topics

- [Digest statistics for MariaDB and MySQL \(p. 628\)](#)
- [Per-second statistics for MariaDB and MySQL \(p. 629\)](#)
- [Per-call statistics for MariaDB and MySQL \(p. 629\)](#)

Digest statistics for MariaDB and MySQL

Performance Insights collects SQL digest statistics from the `events_statements_summary_by_digest` table. The `events_statements_summary_by_digest` table is managed by your database.

The digest table doesn't have an eviction policy. When the table is full, the AWS Management Console shows the following message:

Performance Insights is unable to collect SQL Digest statistics on new queries because the table `events_statements_summary_by_digest` is full.
Please truncate `events_statements_summary_by_digest` table to clear the issue. Check the User Guide for more details.

In this situation, MariaDB and MySQL don't track SQL queries. To address this issue, Performance Insights automatically truncates the digest table when both of the following conditions are met:

- The table is full.
- Performance Insights manages the Performance Schema automatically.

For automatic management, the `performance_schema` parameter must be set to `0` and the **Source** must not be set to `user`. If Performance Insights isn't managing the Performance Schema automatically, see [Turning on the Performance Schema for Performance Insights on Amazon RDS for MariaDB or MySQL \(p. 553\)](#).

In the AWS CLI, check the source of a parameter value by running the `describe-db-parameters` command.

Per-second statistics for MariaDB and MySQL

The following SQL statistics are available for MariaDB and MySQL DB instances.

Metric	Unit
<code>db.sql_tokenized.stats.count_star_per_sec</code>	Calls per second
<code>db.sql_tokenized.stats.sum_timer_wait_per_sec</code>	Average active executions per second (AAE)
<code>db.sql_tokenized.stats.sum_select_full_join_per_sec</code>	Select full join per second
<code>db.sql_tokenized.stats.sum_select_range_check_per_sec</code>	Select range check per second
<code>db.sql_tokenized.stats.sum_select_scan_per_sec</code>	Select scan per second
<code>db.sql_tokenized.stats.sum_sort_merge_passes_per_sec</code>	Sort merge passes per second
<code>db.sql_tokenized.stats.sum_sort_scan_per_sec</code>	Sort scans per second
<code>db.sql_tokenized.stats.sum_sort_range_per_sec</code>	Sort ranges per second
<code>db.sql_tokenized.stats.sum_sort_rows_per_sec</code>	Sort rows per second
<code>db.sql_tokenized.stats.sum_rows_affected_per_sec</code>	Rows affected per second
<code>db.sql_tokenized.stats.sum_rows_examined_per_sec</code>	Rows examined per second
<code>db.sql_tokenized.stats.sum_rows_sent_per_sec</code>	Rows sent per second
<code>db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_sec</code>	Created temporary disk tables per second
<code>db.sql_tokenized.stats.sum_created_tmp_tables_per_sec</code>	Created temporary tables per second
<code>db.sql_tokenized.stats.sum_lock_time_per_sec</code>	Lock time per second (in ms)

Per-call statistics for MariaDB and MySQL

The following metrics provide per call statistics for a SQL statement.

Metric	Unit
<code>db.sql_tokenized.stats.sum_timer_wait_per_call</code>	Average latency per call (in ms)
<code>db.sql_tokenized.stats.sum_select_full_join_per_call</code>	Select full joins per call
<code>db.sql_tokenized.stats.sum_select_range_check_per_call</code>	Select range check per call
<code>db.sql_tokenized.stats.sum_select_scan_per_call</code>	Select scans per call

Metric	Unit
db.sql_tokenized.stats.sum_sort_merge_passes_per_call	Sort merge passes per call
db.sql_tokenized.stats.sum_sort_scan_per_call	Sort scans per call
db.sql_tokenized.stats.sum_sort_range_per_call	Sort ranges per call
db.sql_tokenized.stats.sum_sort_rows_per_call	Sort rows per call
db.sql_tokenized.stats.sum_rows_affected_per_call	Rows affected per call
db.sql_tokenized.stats.sum_rows_examined_per_call	Rows examined per call
db.sql_tokenized.stats.sum_rows_sent_per_call	Rows sent per call
db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_call	Created temporary disk tables per call
db.sql_tokenized.stats.sum_created_tmp_tables_per_call	Created temporary tables per call
db.sql_tokenized.stats.sum_lock_time_per_call	Lock time per call (in ms)

SQL statistics for Oracle

Amazon RDS for Oracle collects SQL statistics both at the statement and digest level. At the statement level, the ID column represents the value of V\$SQL.SQL_ID. At the digest level, the ID column shows the value of V\$SQL.FORCE_MATCHING_SIGNATURE.

If the ID is 0 at the digest level, Oracle Database has determined that this statement is not suitable for reuse. In this case, the child SQL statements could belong to different digests. However, the statements are grouped together under the digest_text for the first SQL statement collected.

Topics

- [Per-second statistics for Oracle \(p. 630\)](#)
- [Per-call statistics for Oracle \(p. 631\)](#)

Per-second statistics for Oracle

The following metrics provide per-second statistics for an Oracle SQL query.

Metric	Unit
db.sql.stats.executions_per_sec	Number of executions per second
db.sql.stats.elapsed_time_per_sec	Average active executions (AAE)
db.sql.stats.rows_processed_per_sec	Rows processed per second
db.sql.stats.buffer_gets_per_sec	Buffer gets per second
db.sql.stats.physical_read_requests_per_sec	Physical reads per second
db.sql.stats.physical_write_requests_per_sec	Physical writes per second
db.sql.stats.total_sharable_mem_per_sec	Total shareable memory per second (in bytes)
db.sql.stats.cpu_time_per_sec	CPU time per second (in ms)

The following metrics provide per-call statistics for an Oracle SQL digest query.

Metric	Unit
db.sql_tokenized.stats.executions_per_sec	Number of executions per second
db.sql_tokenized.stats.elapsed_time_per_sec	Average active executions (AAE)
db.sql_tokenized.stats.rows_processed_per_sec	Rows processed per second
db.sql_tokenized.stats.buffer_gets_per_sec	Buffer gets per second
db.sql_tokenized.stats.physical_read_requests_per_sec	Physical reads per second
db.sql_tokenized.stats.physical_write_requests_per_sec	Physical writes per second
db.sql_tokenized.stats.total_sharable_mem_per_sec	Total shareable memory per second (in bytes)
db.sql_tokenized.stats.cpu_time_per_sec	CPU time per second (in ms)

Per-call statistics for Oracle

The following metrics provide per-call statistics for an Oracle SQL statement.

Metric	Unit
db.sql.stats.elapsed_time_per_exec	Elapsed time per executions (in ms)
db.sql.stats.rows_processed_per_exec	Rows processed per execution
db.sql.stats.buffer_gets_per_exec	Buffer gets per execution
db.sql.stats.physical_read_requests_per_exec	Physical reads per execution
db.sql.stats.physical_write_requests_per_exec	Physical writes per execution
db.sql.stats.total_sharable_mem_per_exec	Total shareable memory per execution (in bytes)
db.sql.stats.cpu_time_per_exec	CPU time per execution (in ms)

The following metrics provide per-call statistics for an Oracle SQL digest query.

Metric	Unit
db.sql_tokenized.stats.elapsed_time_per_exec	Elapsed time per executions (in ms)
db.sql_tokenized.stats.rows_processed_per_exec	Rows processed per execution
db.sql_tokenized.stats.buffer_gets_per_exec	Buffer gets per execution
db.sql_tokenized.stats.physical_read_requests_per_exec	Physical reads per execution
db.sql_tokenized.stats.physical_write_requests_per_exec	Physical writes per execution
db.sql_tokenized.stats.total_sharable_mem_per_exec	Total shareable memory per execution (in bytes)
db.sql_tokenized.stats.cpu_time_per_exec	CPU time per execution (in ms)

SQL statistics for RDS PostgreSQL

For each SQL call and for each second that a query runs, Performance Insights collects SQL statistics. RDS for PostgreSQL collect SQL statistics only at the digest-level. No statistics are shown at the statement-level.

Following, you can find information about digest-level statistics for RDS for PostgreSQL.

Topics

- [Digest statistics for RDS PostgreSQL \(p. 632\)](#)
- [Per-second digest statistics for RDS PostgreSQL \(p. 632\)](#)
- [Per-call digest statistics for RDS PostgreSQL \(p. 633\)](#)

Digest statistics for RDS PostgreSQL

To view SQL digest statistics, RDS PostgreSQL must load the pg_stat_statements library. For PostgreSQL DB instances that are compatible with PostgreSQL 11 or later, the database loads this library by default. For PostgreSQL DB instances that are compatible with PostgreSQL 10 or earlier, enable this library manually. To enable it manually, add pg_stat_statements to shared_preload_libraries in the DB parameter group associated with the DB instance. Then reboot your DB instance. For more information, see [Working with parameter groups \(p. 289\)](#).

Note

Performance Insights can only collect statistics for queries in pg_stat_activity that aren't truncated. By default, PostgreSQL databases truncate queries longer than 1,024 bytes. To increase the query size, change the track_activity_query_size parameter in the DB parameter group associated with your DB instance. When you change this parameter, a DB instance reboot is required.

Per-second digest statistics for RDS PostgreSQL

The following SQL digest statistics are available for PostgreSQL DB instances.

Metric	Unit
db.sql_tokenized.stats.calls_per_sec	Calls per second
db.sql_tokenized.stats.rows_per_sec	Rows per second
db.sql_tokenized.stats.total_time_per_sec	Average active executions per second (AAE)
db.sql_tokenized.stats.shared_blk_hit_per_sec	Block hits per second
db.sql_tokenized.stats.shared_blk_read_per_sec	Block reads per second
db.sql_tokenized.stats.shared_blk_dirtied_per_sec	Blocks dirtied per second
db.sql_tokenized.stats.shared_blk_written_per_sec	Block writes per second
db.sql_tokenized.stats.local_blk_hit_per_sec	Local block hits per second
db.sql_tokenized.stats.local_blk_read_per_sec	Local block reads per second
db.sql_tokenized.stats.local_blk_dirtied_per_sec	Local block dirty per second
db.sql_tokenized.stats.local_blk_written_per_sec	Local block writes per second

Metric	Unit
db.sql_tokenized.stats.temp_blk_written_per_sec	Temporary writes per second
db.sql_tokenized.stats.temp_blk_read_per_sec	Temporary reads per second
db.sql_tokenized.stats.blk_read_time_per_sec	Average concurrent reads per second
db.sql_tokenized.stats.blk_write_time_per_sec	Average concurrent writes per second

Per-call digest statistics for RDS PostgreSQL

The following metrics provide per call statistics for a SQL statement.

Metric	Unit
db.sql_tokenized.stats.rows_per_call	Rows per call
db.sql_tokenized.stats.avg_latency_per_call	Average latency per call (in ms)
db.sql_tokenized.stats.shared_blk_hit_per_call	Block hits per call
db.sql_tokenized.stats.shared_blk_read_per_call	Block reads per call
db.sql_tokenized.stats.shared_blk_written_per_call	Block writes per call
db.sql_tokenized.stats.shared_blk_dirtied_per_call	Blocks dirtied per call
db.sql_tokenized.stats.local_blk_hit_per_call	Local block hits per call
db.sql_tokenized.stats.local_blk_read_per_call	Local block reads per call
db.sql_tokenized.stats.local_blk_dirtied_per_call	Local block dirty per call
db.sql_tokenized.stats.local_blk_written_per_call	Local block writes per call
db.sql_tokenized.stats.temp_blk_written_per_call	Temporary block writes per call
db.sql_tokenized.stats.temp_blk_read_per_call	Temporary block reads per call
db.sql_tokenized.stats.blk_read_time_per_call	Read time per call (in ms)
db.sql_tokenized.stats.blk_write_time_per_call	Write time per call (in ms)

For more information about these metrics, see [pg_stat_statements](#) in the PostgreSQL documentation.

OS metrics in Enhanced Monitoring

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. RDS delivers the metrics from Enhanced Monitoring to your Amazon CloudWatch Logs account. The following tables list the OS metrics available using Amazon CloudWatch Logs.

Topics

- [OS metrics for MariaDB, MySQL, Oracle, and PostgreSQL \(p. 634\)](#)
- [OS metrics for Microsoft SQL Server \(p. 639\)](#)

OS metrics for MariaDB, MySQL, Oracle, and PostgreSQL

Group	Metric	Console name	Description
General	engine	Not applicable	The database engine for the DB instance.
	instanceID	Not applicable	The DB instance identifier.
	instanceResouceID	Not applicable	An immutable identifier for the DB instance that is unique to an AWS Region, also used as the log stream identifier.
	numVCpus	Not applicable	The number of virtual CPUs for the DB instance.
	timestamp	Not applicable	The time at which the metrics were taken.
	uptime	Not applicable	The amount of time that the DB instance has been active.
	version	Not applicable	The version of the OS metrics' stream JSON format.
cpuUtilization	guest	CPU Guest	The percentage of CPU in use by guest programs.
	idle	CPU Idle	The percentage of CPU that is idle.
	irq	CPU IRQ	The percentage of CPU in use by software interrupts.
	nice	CPU Nice	The percentage of CPU in use by programs running at lowest priority.
	steal	CPU Steal	The percentage of CPU in use by other virtual machines.
	system	CPU System	The percentage of CPU in use by the kernel.
	total	CPU Total	The total percentage of the CPU in use. This value includes the nice value.
	user	CPU User	The percentage of CPU in use by user programs.
	wait	CPU Wait	The percentage of CPU unused while waiting for I/O access.
diskIO	avgQueueLen	Avg Queue Size	The number of requests waiting in the I/O device's queue.
	avgReqSz	Ave Request Size	The average request size, in kilobytes.
	await	Disk I/O Await	The number of milliseconds required to respond to requests, including queue time and service time.
	device	Not applicable	The identifier of the disk device in use.
	readIosPS	Read IO/s	The number of read operations per second.

Group	Metric	Console name	Description
read/write metrics	readKb	Read Total	The total number of kilobytes read.
	readKbPS	Read Kb/s	The number of kilobytes read per second.
	readLatency	Read Latency	The elapsed time between the submission of a read I/O request and its completion, in milliseconds. This metric is only available for Amazon Aurora.
	readThroughput	Read Throughput	The amount of network throughput used by requests to the DB cluster, in bytes per second. This metric is only available for Amazon Aurora.
	rrqmPS	Rrqms	The number of merged read requests queued per second.
	tps	TPS	The number of I/O transactions per second.
	util	Disk I/O Util	The percentage of CPU time during which requests were issued.
	writeI0sPS	Write IO/s	The number of write operations per second.
	writeKb	Write Total	The total number of kilobytes written.
	writeKbPS	Write Kb/s	The number of kilobytes written per second.
	writeLatency	Write Latency	The average elapsed time between the submission of a write I/O request and its completion, in milliseconds. This metric is only available for Amazon Aurora.
	writeThroughput	Write Throughput	The amount of network throughput used by responses from the DB cluster, in bytes per second. This metric is only available for Amazon Aurora.
	wrqmPS	Wrqms	The number of merged write requests queued per second.
physicalDevice metrics	ioQueueLen	Physical Devices Avg Queue Size	The number of requests waiting in the I/O device's queue.
	avgReqSz	Physical Devices Ave Request Size	The average request size, in kilobytes.
	await	Physical Devices Disk I/O Await	The number of milliseconds required to respond to requests, including queue time and service time.
	device	Not applicable	The identifier of the disk device in use.
	readI0sPS	Physical Devices Read IO/s	The number of read operations per second.

Group	Metric	Console name	Description
	readKb	Physical Devices Read Total	The total number of kilobytes read.
	readKbPS	Physical Devices Read Kb/s	The number of kilobytes read per second.
	rrqmPS	Physical Devices Rrqms	The number of merged read requests queued per second.
	tps	Physical Devices TPS	The number of I/O transactions per second.
	util	Physical Devices Disk I/O Util	The percentage of CPU time during which requests were issued.
	writeI0sPS	Physical Devices Write IO/s	The number of write operations per second.
	writeKb	Physical Devices Write Total	The total number of kilobytes written.
	writeKbPS	Physical Devices Write Kb/s	The number of kilobytes written per second.
	wrqmPS	Physical Devices Wrqms	The number of merged write requests queued per second.
fileSys	maxFiles	Max Inodes	The maximum number of files that can be created for the file system.
	mountPoint	Not applicable	The path to the file system.
	name	Not applicable	The name of the file system.
	total	Total Filesystem	The total number of disk space available for the file system, in kilobytes.
	used	Used Filesystem	The amount of disk space used by files in the file system, in kilobytes.
	usedFilePercent	Used %	The percentage of available files in use.
	usedFiles	Used Inodes	The number of files in the file system.
	usedPercent	Used Inodes %	The percentage of the file-system disk space in use.

Group	Metric	Console name	Description
loadAverage	fifteen	Load Avg 15 min	The number of processes requesting CPU time over the last 15 minutes.
	five	Load Avg 5 min	The number of processes requesting CPU time over the last 5 minutes.
	one	Load Avg 1 min	The number of processes requesting CPU time over the last minute.
memory	active	Active Memory	The amount of assigned memory, in kilobytes.
	buffers	Buffered Memory	The amount of memory used for buffering I/O requests prior to writing to the storage device, in kilobytes.
	cached	Cached Memory	The amount of memory used for caching file system-based I/O.
	dirty	Dirty Memory	The amount of memory pages in RAM that have been modified but not written to their related data block in storage, in kilobytes.
	free	Free Memory	The amount of unassigned memory, in kilobytes.
	hugePagesFree	Huge Pages Free	The number of free huge pages. Huge pages are a feature of the Linux kernel.
	hugePagesRsvd	Huge Pages Rsvd	The number of committed huge pages.
	hugePagesSz	Huge Pages Size	The size for each huge pages unit, in kilobytes.
	hugePagesSurp	Huge Pages Surp	The number of available surplus huge pages over the total.
	hugePagesTotal	Huge Pages Total	The total number of huge pages.
	inactive	Inactive Memory	The amount of least-frequently used memory pages, in kilobytes.
	mapped	Mapped Memory	The total amount of file-system contents that is memory mapped inside a process address space, in kilobytes.
	pageTables	Page Tables	The amount of memory used by page tables, in kilobytes.
	slab	Slab Memory	The amount of reusable kernel data structures, in kilobytes.
	total	Total Memory	The total amount of memory, in kilobytes.
	writeback	Writeback Memory	The amount of dirty pages in RAM that are still being written to the backing storage, in kilobytes.

Group	Metric	Console name	Description
network	interface	Not applicable	The identifier for the network interface being used for the DB instance.
	rx	RX	The number of bytes received per second.
	tx	TX	The number of bytes uploaded per second.
processList	cpuUsedPc	CPU %	The percentage of CPU used by the process.
	id	Not applicable	The identifier of the process.
	memoryUsedPc	MEM%	The percentage of memory used by the process.
	name	Not applicable	The name of the process.
	parentID	Not applicable	The process identifier for the parent process of the process.
	rss	RES	The amount of RAM allocated to the process, in kilobytes.
	tgid	Not applicable	The thread group identifier, which is a number representing the process ID to which a thread belongs. This identifier is used to group threads from the same process.
	vss	VIRT	The amount of virtual memory allocated to the process, in kilobytes.
swap	swap	Swap	The amount of swap memory available, in kilobytes.
	swap_in	Swaps in	The amount of memory, in kilobytes, swapped in from disk.
	swap_out	Swaps out	The amount of memory, in kilobytes, swapped out to disk.
	free	Free Swap	The amount of swap memory free, in kilobytes.
	committed	Committed Swap	The amount of swap memory, in kilobytes, used as cache memory.
tasks	blocked	Tasks Blocked	The number of tasks that are blocked.
	running	Tasks Running	The number of tasks that are running.
	sleeping	Tasks Sleeping	The number of tasks that are sleeping.
	stopped	Tasks Stopped	The number of tasks that are stopped.
	total	Tasks Total	The total number of tasks.

Group	Metric	Console name	Description
	zombie	Tasks Zombie	The number of child tasks that are inactive with an active parent task.

OS metrics for Microsoft SQL Server

Group	Metric	Console name	Description
General	engine	Not applicable	The database engine for the DB instance.
	instanceID	Not applicable	The DB instance identifier.
	instanceResourceIdentifier	Not applicable	An immutable identifier for the DB instance that is unique to an AWS Region, also used as the log stream identifier.
	numVCpus	Not applicable	The number of virtual CPUs for the DB instance.
	timestamp	Not applicable	The time at which the metrics were taken.
	uptime	Not applicable	The amount of time that the DB instance has been active.
	version	Not applicable	The version of the OS metrics' stream JSON format.
cpuUtilization	idle	CPU Idle	The percentage of CPU that is idle.
	kern	CPU Kernel	The percentage of CPU in use by the kernel.
	user	CPU User	The percentage of CPU in use by user programs.
disks	name	Not applicable	The identifier for the disk.
	totalKb	Total Disk Space	The total space of the disk, in kilobytes.
	usedKb	Used Disk Space	The amount of space used on the disk, in kilobytes.
	usedPc	Used Disk Space %	The percentage of space used on the disk.
	availKb	Available Disk Space	The space available on the disk, in kilobytes.
	availPc	Available Disk Space %	The percentage of space available on the disk.
	rdCountPS	Reads/s	The number of read operations per second
	rdBytesPS	Read Kb/s	The number of bytes read per second.
	wrCountPS	Write IO/s	The number of write operations per second.
	wrBytesPS	Write Kb/s	The amount of bytes written per second.

Group	Metric	Console name	Description
memory	commitTotKb	Commit Total	The amount of pagefile-backed virtual address space in use, that is, the current commit charge. This value is composed of main memory (RAM) and disk (pagefiles).
	commitLimitKb	Maximum Commit	The maximum possible value for the commitTotKb metric. This value is the sum of the current pagefile size plus the physical memory available for pageable contents, excluding RAM that is assigned to nonpageable areas.
	commitPeakKb	Commit Peak	The largest value of the commitTotKb metric since the operating system was last started.
	kernTotKb	Total Kernel Memory	The sum of the memory in the paged and nonpaged kernel pools, in kilobytes.
	kernPagedKb	Paged Kernel Memory	The amount of memory in the paged kernel pool, in kilobytes.
	kernNonpagedKb	Nonpaged Kerenel Memory	The amount of memory in the nonpaged kernel pool, in kilobytes.
	pageSize	Page Size	The size of a page, in bytes.
	physTotKb	Total Memory	The amount of physical memory, in kilobytes.
	physAvailKb	Available Memory	The amount of available physical memory, in kilobytes.
	sqlServerTotKb	SQL Server Total Memory	The amount of memory committed to SQL Server, in kilobytes.
network	sysCacheKb	System Cache	The amount of system cache memory, in kilobytes.
	interface	Not applicable	The identifier for the network interface being used for the DB instance.
	rdBytesPS	Network Read Kb/s	The number of bytes received per second.
processList	wrBytesPS	Network Write Kb/s	The number of bytes sent per second.
	cpuUsedPc	Used %	The percentage of CPU used by the process.
	memUsedPc	MEM%	The percentage of total memory used by the process.
	name	Not applicable	The name of the process.
	pid	Not applicable	The identifier of the process. This value is not present for processes that are owned by Amazon RDS.

Group	Metric	Console name	Description
	ppid	Not applicable	The process identifier for the parent of this process. This value is only present for child processes.
	tid	Not applicable	The thread identifier. This value is only present for threads. The owning process can be identified by using the pid value.
	workingSetKb	Not applicable	The amount of memory in the private working set plus the amount of memory that is in use by the process and can be shared with other processes, in kilobytes.
	workingSetPrivKb	Not applicable	The amount of memory that is in use by a process, but can't be shared with other processes, in kilobytes.
	workingSetSharedKb	Not applicable	The amount of memory that is in use by a process and can be shared with other processes, in kilobytes.
	virtKb	Not applicable	The amount of virtual address space the process is using, in kilobytes. Use of virtual address space doesn't necessarily imply corresponding use of either disk or main memory pages.
system	handles	Handles	The number of handles that the system is using.
	processes	Processes	The number of processes running on the system.
	threads	Threads	The number of threads running on the system.

Monitoring events, logs, and streams in an Amazon RDS DB instance

When you monitor your Amazon RDS databases and your other AWS solutions, your goal is to maintain the following:

- Reliability
- Availability
- Performance
- Security

[Monitoring metrics in an Amazon RDS instance \(p. 510\)](#) explains how to monitor your instance using metrics. A complete solution must also monitor database events, log files, and activity streams. AWS provides you with the following monitoring tools:

- *Amazon EventBridge* is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, Software-as-a-Service (SaaS) applications, and AWS services. EventBridge routes that data to targets such as AWS Lambda. This way, you can monitor events that happen in services and build event-driven architectures. For more information, see the [Amazon EventBridge User Guide](#).
- *Amazon CloudWatch Logs* provides a way to monitor, store, and access your log files from Amazon RDS instances, AWS CloudTrail, and other sources. Amazon CloudWatch Logs can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the [Amazon CloudWatch Logs User Guide](#).
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account. CloudTrail delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the [AWS CloudTrail User Guide](#).
- *Database Activity Streams* is an Amazon RDS feature that provides a near real-time stream of the activity in your Oracle DB instance. Amazon RDS pushes activities to an Amazon Kinesis data stream. The Kinesis stream is created automatically. From Kinesis, you can configure AWS services such as Amazon Kinesis Data Firehose and AWS Lambda to consume the stream and store the data.

Topics

- [Viewing logs, events, and streams in the Amazon RDS console \(p. 642\)](#)
- [Monitoring Amazon RDS events \(p. 646\)](#)
- [Monitoring Amazon RDS log files \(p. 680\)](#)
- [Monitoring Amazon RDS API calls in AWS CloudTrail \(p. 725\)](#)
- [Monitoring Amazon RDS for Oracle with Database Activity Streams \(p. 729\)](#)

Viewing logs, events, and streams in the Amazon RDS console

Amazon RDS integrates with AWS services to show information about logs, events, and database activity streams in the RDS console.

The **Logs & events** tab for your RDS DB instance shows the following information:

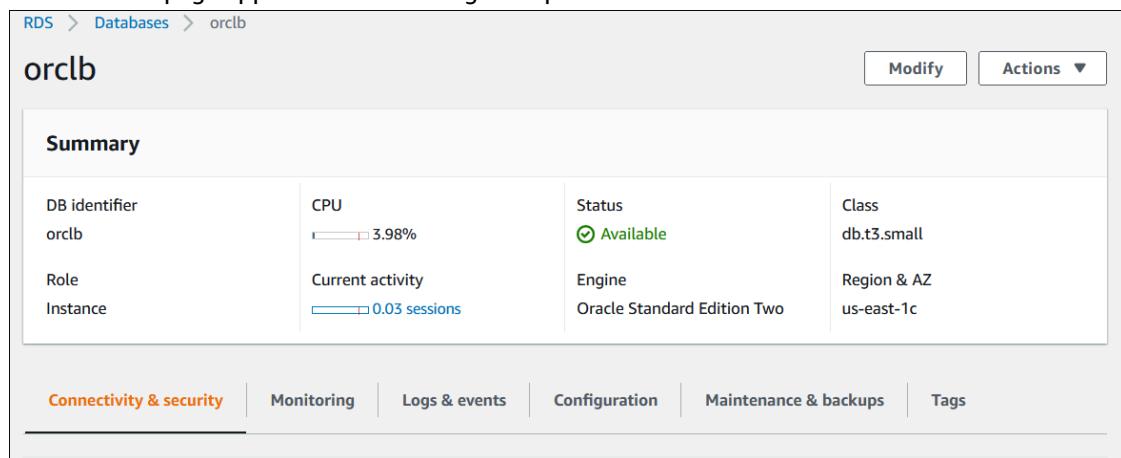
- **Amazon CloudWatch alarms** – Shows any metric alarms that you have configured for the DB instance. If you haven't configured alarms, you can create them in the RDS console. For more information, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#).
- **Recent events** – Shows a summary of events (environment changes) for your RDS DB instance . For more information, see [Viewing Amazon RDS events \(p. 647\)](#).
- **Logs** – Shows database log files generated by a DB instance. For more information, see [Monitoring Amazon RDS log files \(p. 680\)](#).

The **Configuration** tab displays information about database activity streams.

To view logs, events, and streams for your DB instance in the RDS console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that you want to monitor.

The database page appears. The following example shows an Oracle database named orclb.



4. Choose **Logs & events**.

The Logs & events section appears.

The screenshot shows the 'Logs & events' section of the Amazon RDS console. It includes three main sections: 'CloudWatch alarms (0)', 'Recent events (2)', and 'Logs (1478)'. Each section has a search bar, a table header, and a list of items with details.

CloudWatch alarms (0)

Name	State	More options
Empty alarms table		
Create alarm		

Recent events (2)

Time	System notes
February 04, 2022, 10:01:40 AM UTC	Backing up DB instance
February 04, 2022, 10:05:26 AM UTC	Finished DB Instance backup

Logs (1478)

Name	Last written	Logs
audit/ORCLB_j001_23080_20220202220030509284475170.aud	Wed Feb 02 2022 17:01:09 GMT-0500	649.6 kB
audit/ORCLB_j003_450_2022020322001748233361498.aud	Thu Feb 03 2022 17:00:32 GMT-0500	537.7 kB

5. Choose Configuration.

The following example shows the status of the database activity streams for your RDS for Oracle DB instance.

Configuration	Maintenance & backups	Tags
Storage	Performance Insights	
Encryption	Performance Insights enabled	
Not enabled	Yes	
Storage type	AWS KMS key	
General Purpose SSD (gp2)	aws/rds	
Provisioned IOPS	Retention period	
-	731 days	
Storage	Published logs	
98 GiB	CloudWatch Logs	
Storage autoscaling	Alert	
Enabled	Audit	
Maximum storage threshold	Listener	
1000 GiB	Trace	
	Database activity stream	
	Status	
	 Stopped	

Monitoring Amazon RDS events

An *event* indicates a change in an environment. This can be an AWS environment, an SaaS partner service or application, or a custom application or service. For descriptions of the RDS events, see [Amazon RDS event categories and event messages \(p. 668\)](#).

Topics

- [Overview of events for Amazon RDS \(p. 646\)](#)
- [Viewing Amazon RDS events \(p. 647\)](#)
- [Working with Amazon RDS event notification \(p. 650\)](#)
- [Creating a rule that triggers on an Amazon RDS event \(p. 664\)](#)
- [Amazon RDS event categories and event messages \(p. 668\)](#)

Overview of events for Amazon RDS

An *RDS event* indicates a change in the Amazon RDS environment. For example, Amazon RDS generates an event when the state of a DB instance changes from pending to running. Amazon RDS delivers events to CloudWatch Events and EventBridge in near-real time.

Note

Amazon RDS emits events on a best effort basis. We recommend that you avoid writing programs that depend on the order or existence of notification events, because they might be out of sequence or missing.

Amazon RDS records events that relate to the following resources:

- DB instances
 - For a list of DB instance events, see [DB instance events \(p. 669\)](#).
- DB parameter groups
 - For a list of DB parameter group events, see [DB parameter group events \(p. 676\)](#).
- DB security groups
 - For a list of DB security group events, see [DB security group events \(p. 676\)](#).
- DB snapshots
 - For a list of DB snapshot events, see [DB snapshot events \(p. 677\)](#).
- RDS Proxy events
 - For a list of RDS Proxy events, see [RDS Proxy events \(p. 678\)](#).

This information includes the following:

- The date and time of the event
- The source name and source type of the event
- A message associated with the event

Viewing Amazon RDS events

You can retrieve the following event information for your Amazon RDS resources:

- Resource name
- Resource type
- Time of the event
- Message summary of the event

Access the events through the AWS Management Console, which shows events from the past 24 hours. You can also retrieve events by using the [describe-events](#) AWS CLI command, or the [DescribeEvents](#) RDS API operation. If you use the AWS CLI or the RDS API to view events, you can retrieve events for up to the past 14 days.

Note

If you need to store events for longer periods of time, you can send Amazon RDS events to CloudWatch Events. For more information, see [Creating a rule that triggers on an Amazon RDS event \(p. 664\)](#)

For descriptions of the Amazon RDS events, see [Amazon RDS event categories and event messages \(p. 668\)](#).

To access detailed information about events using AWS CloudTrail, including request parameters, see [CloudTrail events \(p. 725\)](#).

Console

To view all Amazon RDS events for the past 24 hours

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Events**.

The available events appear in a list.

3. (Optional) Enter a search term to filter your results.

The following example shows a list of events filtered by the characters **stopped**.

Source	Type	Time	Message
orclb	Instances	March 19, 2021, 7:34:09 PM UTC	DB instance stopped

AWS CLI

To view all events generated in the last hour, call [describe-events](#) with no parameters.

```
aws rds describe-events
```

The following sample output shows that a DB instance has been stopped.

```
{  
    "Events": [  
        {  
            "EventCategories": [  
                "notification"  
            ],  
            "SourceType": "db-instance",  
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:testinst",  
            "Date": "2022-04-22T21:31:00.681Z",  
            "Message": "DB instance stopped",  
            "SourceIdentifier": "testinst"  
        }  
    ]  
}
```

To view all Amazon RDS events for the past 10080 minutes (7 days), call the [describe-events](#) AWS CLI command and set the --duration parameter to 10080.

```
aws rds describe-events --duration 10080
```

The following example shows the events in the specified time range for DB instance *test-instance*.

```
aws rds describe-events \  
    --source-identifier test-instance \  
    --source-type db-instance \  
    --start-time 2022-03-13T22:00Z \  
    --end-time 2022-03-13T23:59Z
```

The following sample output shows the status of a backup.

```
{  
    "Events": [  
        {  
            "SourceType": "db-instance",  
            "SourceIdentifier": "test-instance",  
            "EventCategories": [  
                "backup"  
            ],  
            "Message": "Backing up DB instance",  
            "Date": "2022-03-13T23:09:23.983Z",  
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"  
        },  
        {  
            "SourceType": "db-instance",  
            "SourceIdentifier": "test-instance",  
            "EventCategories": [  
                "backup"  
            ],  
            "Message": "Finished DB Instance backup",  
            "Date": "2022-03-13T23:15:13.049Z",  
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"  
        }  
    ]  
}
```

API

You can view all Amazon RDS instance events for the past 14 days by calling the [DescribeEvents](#) RDS API operation and setting the `Duration` parameter to 20160.

Working with Amazon RDS event notification

Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs. These notifications can be in any notification form supported by Amazon SNS for an AWS Region, such as an email, a text message, or a call to an HTTP endpoint.

Topics

- [Overview of Amazon RDS event notification \(p. 650\)](#)
- [Granting permissions to publish notifications to an Amazon SNS topic \(p. 654\)](#)
- [Subscribing to Amazon RDS event notification \(p. 655\)](#)
- [Listing Amazon RDS event notification subscriptions \(p. 658\)](#)
- [Modifying an Amazon RDS event notification subscription \(p. 659\)](#)
- [Adding a source identifier to an Amazon RDS event notification subscription \(p. 660\)](#)
- [Removing a source identifier from an Amazon RDS event notification subscription \(p. 661\)](#)
- [Listing the Amazon RDS event notification categories \(p. 662\)](#)
- [Deleting an Amazon RDS event notification subscription \(p. 663\)](#)

Overview of Amazon RDS event notification

Amazon RDS groups events into categories that you can subscribe to so that you can be notified when an event in that category occurs.

Topics

- [RDS resources eligible for event subscription \(p. 650\)](#)
- [Basic process for subscribing to Amazon RDS event notifications \(p. 651\)](#)
- [Delivery of RDS event notifications \(p. 651\)](#)
- [Billing for Amazon RDS event notifications \(p. 651\)](#)
- [Examples of Amazon RDS events \(p. 651\)](#)

RDS resources eligible for event subscription

You can subscribe to an event category for the following resources:

- DB instance
- DB snapshot
- DB parameter group
- DB security group
- RDS Proxy
- Custom engine version

For example, if you subscribe to the backup category for a given DB instance, you're notified whenever a backup-related event occurs that affects the DB instance. If you subscribe to a configuration change category for a DB instance, you're notified when the DB instance is changed. You also receive notification when an event notification subscription changes.

You might want to create several different subscriptions. For example, you might create one subscription that receives all event notifications for all DB instances and another subscription that includes only critical events for a subset of the DB instances. For the second subscription, specify one or more DB instances in the filter.

Basic process for subscribing to Amazon RDS event notifications

The process for subscribing to Amazon RDS event notification is as follows:

1. You create an Amazon RDS event notification subscription by using the Amazon RDS console, AWS CLI, or API.

Amazon RDS uses the ARN of an Amazon SNS topic to identify each subscription. The Amazon RDS console creates the ARN for you when you create the subscription. Create the ARN by using the Amazon SNS console, the AWS CLI, or the Amazon SNS API.
2. Amazon RDS sends an approval email or SMS message to the addresses you submitted with your subscription.
3. You confirm your subscription by choosing the link in the notification you received.
4. The Amazon RDS console updates the **My Event Subscriptions** section with the status of your subscription.
5. Amazon RDS begins sending the notifications to the addresses that you provided when you created the subscription.

To learn about identity and access management when using Amazon SNS, see [Identity and access management in Amazon SNS](#) in the *Amazon Simple Notification Service Developer Guide*.

You can use AWS Lambda to process event notifications from a DB instance. For more information, see [Using AWS Lambda with Amazon RDS](#) in the *AWS Lambda Developer Guide*.

Delivery of RDS event notifications

Amazon RDS sends notifications to the addresses that you provide when you create the subscription. The notification can include message attributes which provide structured metadata about the message. For more information about message attributes, see [Amazon RDS event categories and event messages \(p. 668\)](#).

Event notifications might take up to five minutes to be delivered.

Important

Amazon RDS doesn't guarantee the order of events sent in an event stream. The event order is subject to change.

When Amazon SNS sends a notification to a subscribed HTTP or HTTPS endpoint, the POST message sent to the endpoint has a message body that contains a JSON document. For more information, see [Amazon SNS message and JSON formats](#) in the *Amazon Simple Notification Service Developer Guide*.

You can configure SNS to notify you with text messages. For more information, see [Mobile text messaging \(SMS\)](#) in the *Amazon Simple Notification Service Developer Guide*.

To turn off notifications without deleting a subscription, choose **No** for **Enabled** in the Amazon RDS console. Or you can set the Enabled parameter to false using the AWS CLI or Amazon RDS API.

Billing for Amazon RDS event notifications

Billing for Amazon RDS event notification is through Amazon SNS. Amazon SNS fees apply when using event notification. For more information about Amazon SNS billing, see [Amazon Simple Notification Service pricing](#).

Examples of Amazon RDS events

The following examples illustrate different types of Amazon RDS events in JSON format. For a tutorial that shows you how to capture and view events in JSON format, see [Tutorial: Log DB instance state changes using Amazon EventBridge \(p. 665\)](#).

Topics

- [Example of a DB instance event \(p. 652\)](#)
- [Example of a DB parameter group event \(p. 652\)](#)
- [Example of a DB snapshot event \(p. 653\)](#)

Example of a DB instance event

The following is an example of a DB instance event in JSON format. The event shows that RDS performed a multi-AZ failover for the instance named my-db-instance. The event ID is RDS-EVENT-0049.

```
{  
    "version": "0",  
    "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ffd4e",  
    "detail-type": "RDS DB Instance Event",  
    "source": "aws.rds",  
    "account": "123456789012",  
    "time": "2018-09-27T22:36:43Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:rds:us-east-1:123456789012:db:my-db-instance"  
    ],  
    "detail": {  
        "EventCategories": [  
            "failover"  
        ],  
        "SourceType": "DB_INSTANCE",  
        "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",  
        "Date": "2018-09-27T22:36:43.292Z",  
        "Message": "A Multi-AZ failover has completed.",  
        "SourceIdentifier": "rds:my-db-instance",  
        "EventID": "RDS-EVENT-0049"  
    }  
}
```

Example of a DB parameter group event

The following is an example of a DB parameter group event in JSON format. The event shows that the parameter time_zone was updated in parameter group my-db-param-group. The event ID is RDS-EVENT-0037.

```
{  
    "version": "0",  
    "id": "844e2571-85d4-695f-b930-0153b71dc42",  
    "detail-type": "RDS DB Parameter Group Event",  
    "source": "aws.rds",  
    "account": "123456789012",  
    "time": "2018-10-06T12:26:13Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group"  
    ],  
    "detail": {  
        "EventCategories": [  
            "configuration change"  
        ],  
        "SourceType": "DB_PARAM",  
        "SourceArn": "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group",  
        "Date": "2018-10-06T12:26:13.882Z",  
        "Message": "Updated parameter time_zone to UTC with apply method immediate",  
    }  
}
```

```
        "SourceIdentifier": "rds:my-db-param-group",
        "EventID": "RDS-EVENT-0037"
    }
```

Example of a DB snapshot event

The following is an example of a DB snapshot event in JSON format. The event shows the deletion of the snapshot named my-db-snapshot. The event ID is RDS-EVENT-0041.

```
{
    "version": "0",
    "id": "844e2571-85d4-695f-b930-0153b71dcb42",
    "detail-type": "RDS DB Snapshot Event",
    "source": "aws.rds",
    "account": "123456789012",
    "time": "2018-10-06T12:26:13Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:rds:us-east-1:123456789012:snapshot:rds:my-db-snapshot"
    ],
    "detail": {
        "EventCategories": [
            "deletion"
        ],
        "SourceType": "SNAPSHOT",
        "SourceArn": "arn:aws:rds:us-east-1:123456789012:snapshot:rds:my-db-snapshot",
        "Date": "2018-10-06T12:26:13.882Z",
        "Message": "Deleted manual snapshot",
        "SourceIdentifier": "rds:my-db-snapshot",
        "EventID": "RDS-EVENT-0041"
    }
}
```

Granting permissions to publish notifications to an Amazon SNS topic

To grant Amazon RDS permissions to publish notifications to an Amazon Simple Notification Service (Amazon SNS) topic, attach an AWS Identity and Access Management (IAM) policy to the destination topic. For more information about permissions, see [Example cases for Amazon Simple Notification Service access control](#) in the *Amazon Simple Notification Service Developer Guide*.

By default, an Amazon SNS topic has a policy allowing all Amazon RDS resources within the same account to publish notifications to it. You can attach a custom policy to allow cross-account notifications, or to restrict access to certain resources.

The following is an example of an IAM policy that you attach to the destination Amazon SNS topic. It restricts the topic to DB instances with names that match the specified prefix. To use this policy, specify the following values:

- Resource – The Amazon Resource Name (ARN) for your Amazon SNS topic
- SourceARN – Your RDS resource ARN
- SourceAccount – Your AWS account ID

To see a list of resource types and their ARNs, see [Resources Defined by Amazon RDS](#) in the *Service Authorization Reference*.

```
{  
    "Version": "2008-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "events.rds.amazonaws.com"  
            },  
            "Action": [  
                "sns:Publish"  
            ],  
            "Resource": "arn:aws:sns:us-east-1:123456789012:topic_name",  
            "Condition": {  
                "ArnLike": {  
                    "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:prefix-*"  
                },  
                "StringEquals": {  
                    "aws:SourceAccount": "123456789012"  
                }  
            }  
        }  
    ]  
}
```

Subscribing to Amazon RDS event notification

The simplest way to create a subscription is with the RDS console. If you choose to create event notification subscriptions using the CLI or API, you must create an Amazon Simple Notification Service topic and subscribe to that topic with the Amazon SNS console or Amazon SNS API. You will also need to retain the Amazon Resource Name (ARN) of the topic because it is used when submitting CLI commands or API operations. For information on creating an SNS topic and subscribing to it, see [Getting started with Amazon SNS](#) in the *Amazon Simple Notification Service Developer Guide*.

You can specify the type of source you want to be notified of and the Amazon RDS source that triggers the event:

Source type

The type of source. For example, **Source type** might be **Instances**. You must choose a source type.

Resources to include

The Amazon RDS resources that are generating the events. For example, you might choose **Select specific instances** and then **myDBInstance1**.

The following table explains the result when you specify or don't specify **Resources to include**.

Resources to include	Description	Example
Specified	RDS notifies you about all events for the specified resource only.	If your Source type is Instances and your resource is myDBInstance1 , RDS notifies you about all events for myDBInstance1 only.
Not specified	RDS notifies you about the events for the specified source type for all your Amazon RDS resources.	If your Source type is Instances , RDS notifies you about all instance-related events in your account.

Console

To subscribe to RDS event notification

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In navigation pane, choose **Event subscriptions**.
3. In the **Event subscriptions** pane, choose **Create event subscription**.
4. Enter your subscription details as follows:
 - a. For **Name**, enter a name for the event notification subscription.
 - b. For **Send notifications to**, do one of the following:
 - Choose **New email topic**. Enter a name for your email topic and a list of recipients.
 - Choose **Amazon Resource Name (ARN)**. Then choose existing Amazon SNS ARN for an Amazon SNS topic.

If you want to use a topic that has been enabled for server-side encryption (SSE), grant Amazon RDS the necessary permissions to access the AWS KMS key. For more information, see

Enable compatibility between event sources from AWS services and encrypted topics in the *Amazon Simple Notification Service Developer Guide*.

- c. For **Source type**, choose a source type. For example, choose **Instances** or **Parameter groups**.
- d. Choose the event categories and resources that you want to receive event notifications for.

The following example configures event notifications for the DB instance named testinst.

The screenshot shows the 'Source' configuration dialog. It includes fields for 'Source type' (set to 'Instances'), 'Instances to include' (set to 'Select specific instances' with 'testinst' selected), and 'Event categories to include' (set to 'All event categories').

- e. Choose **Create**.

The Amazon RDS console indicates that the subscription is being created.

Event subscriptions (2)				
		Edit	Delete	Create event subscription
<input type="text"/> Filter event subscriptions				
Name	Status	Source Type	Enabled	
Configchangerdpgres	active	Instances	Yes	
Test	creating	Instances	Yes	

AWS CLI

To subscribe to RDS event notification, use the AWS CLI [create-event-subscription](#) command. Include the following required parameters:

- `--subscription-name`
- `--sns-topic-arn`

Example

For Linux, macOS, or Unix:

```
aws rds create-event-subscription \
--subscription-name myeventsSubscription \
--sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS \
--enabled
```

For Windows:

```
aws rds create-event-subscription ^
--subscription-name myeventsubscription ^
--sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS ^
--enabled
```

API

To subscribe to Amazon RDS event notification, call the Amazon RDS API function [CreateEventSubscription](#). Include the following required parameters:

- `SubscriptionName`
- `SnsTopicArn`

Listings Amazon RDS event notification subscriptions

You can list your current Amazon RDS event notification subscriptions.

Console

To list your current Amazon RDS event notification subscriptions

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Event subscriptions**. The **Event subscriptions** pane shows all your event notification subscriptions.

Event subscriptions (2)		
	Name	Status
<input type="checkbox"/> <input type="checkbox"/> Filter event subscriptions		
<input type="checkbox"/>	Configchangerdpgres	active
<input type="checkbox"/>	Postgresnotification	active

AWS CLI

To list your current Amazon RDS event notification subscriptions, use the AWS CLI [describe-event-subscriptions](#) command.

Example

The following example describes all event subscriptions.

```
aws rds describe-event-subscriptions
```

The following example describes the *myfirsteventsubscription*.

```
aws rds describe-event-subscriptions --subscription-name myfirsteventsubscription
```

API

To list your current Amazon RDS event notification subscriptions, call the Amazon RDS API [DescribeEventSubscriptions](#) action.

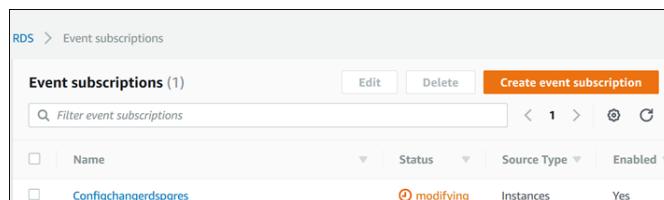
Modifying an Amazon RDS event notification subscription

After you have created a subscription, you can change the subscription name, source identifier, categories, or topic ARN.

Console

To modify an Amazon RDS event notification subscription

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Event subscriptions**.
3. In the **Event subscriptions** pane, choose the subscription that you want to modify and choose **Edit**.
4. Make your changes to the subscription in either the **Target** or **Source** section.
5. Choose **Edit**. The Amazon RDS console indicates that the subscription is being modified.



AWS CLI

To modify an Amazon RDS event notification subscription, use the AWS CLI `modify-event-subscription` command. Include the following required parameter:

- `--subscription-name`

Example

The following code enables `myeventsSubscription`.

For Linux, macOS, or Unix:

```
aws rds modify-event-subscription \
--subscription-name myeventsSubscription \
--enabled
```

For Windows:

```
aws rds modify-event-subscription ^
--subscription-name myeventsSubscription ^
--enabled
```

API

To modify an Amazon RDS event, call the Amazon RDS API operation `ModifyEventSubscription`. Include the following required parameter:

- `SubscriptionName`

Adding a source identifier to an Amazon RDS event notification subscription

You can add a source identifier (the Amazon RDS source generating the event) to an existing subscription.

Console

You can easily add or remove source identifiers using the Amazon RDS console by selecting or deselecting them when modifying a subscription. For more information, see [Modifying an Amazon RDS event notification subscription \(p. 659\)](#).

AWS CLI

To add a source identifier to an Amazon RDS event notification subscription, use the AWS CLI [add-source-identifier-to-subscription](#) command. Include the following required parameters:

- `--subscription-name`
- `--source-identifier`

Example

The following example adds the source identifier `mysqldb` to the `myrdseventsSubscription` subscription.

For Linux, macOS, or Unix:

```
aws rds add-source-identifier-to-subscription \
  --subscription-name myrdseventsSubscription \
  --source-identifier mysqldb
```

For Windows:

```
aws rds add-source-identifier-to-subscription ^
  --subscription-name myrdseventsSubscription ^
  --source-identifier mysqldb
```

API

To add a source identifier to an Amazon RDS event notification subscription, call the Amazon RDS API [AddSourceIdentifierToSubscription](#). Include the following required parameters:

- `SubscriptionName`
- `SourceIdentifier`

Removing a source identifier from an Amazon RDS event notification subscription

You can remove a source identifier (the Amazon RDS source generating the event) from a subscription if you no longer want to be notified of events for that source.

Console

You can easily add or remove source identifiers using the Amazon RDS console by selecting or deselecting them when modifying a subscription. For more information, see [Modifying an Amazon RDS event notification subscription \(p. 659\)](#).

AWS CLI

To remove a source identifier from an Amazon RDS event notification subscription, use the AWS CLI `remove-source-identifier-from-subscription` command. Include the following required parameters:

- `--subscription-name`
- `--source-identifier`

Example

The following example removes the source identifier `mysql ldb` from the `myrdseventssubscription` subscription.

For Linux, macOS, or Unix:

```
aws rds remove-source-identifier-from-subscription \
  --subscription-name myrdseventssubscription \
  --source-identifier mysql ldb
```

For Windows:

```
aws rds remove-source-identifier-from-subscription ^
  --subscription-name myrdseventssubscription ^
  --source-identifier mysql ldb
```

API

To remove a source identifier from an Amazon RDS event notification subscription, use the Amazon RDS API `RemoveSourceIdentifierFromSubscription` command. Include the following required parameters:

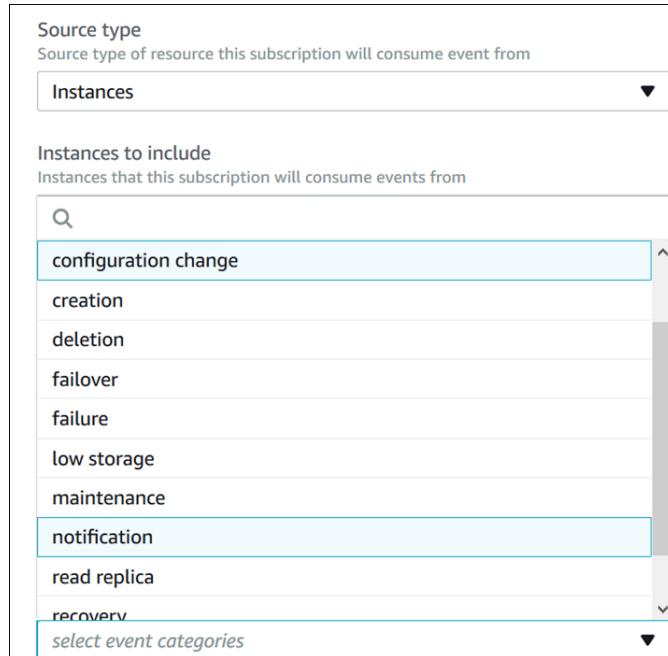
- `SubscriptionName`
- `SourceIdentifier`

List the Amazon RDS event notification categories

All events for a resource type are grouped into categories. To view the list of categories available, use the following procedures.

Console

When you create or modify an event notification subscription, the event categories are displayed in the Amazon RDS console. For more information, see [Modifying an Amazon RDS event notification subscription \(p. 659\)](#).



AWS CLI

To list the Amazon RDS event notification categories, use the AWS CLI [describe-event-categories](#) command. This command has no required parameters.

Example

```
aws rds describe-event-categories
```

API

To list the Amazon RDS event notification categories, use the Amazon RDS API [DescribeEventCategories](#) command. This command has no required parameters.

Deleting an Amazon RDS event notification subscription

You can delete a subscription when you no longer need it. All subscribers to the topic will no longer receive event notifications specified by the subscription.

Console

To delete an Amazon RDS event notification subscription

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **DB Event Subscriptions**.
3. In the **My DB Event Subscriptions** pane, choose the subscription that you want to delete.
4. Choose **Delete**.
5. The Amazon RDS console indicates that the subscription is being deleted.

The screenshot shows the 'Event subscriptions' section of the Amazon RDS console. It displays two entries in a table:

Name	Status
Configchangerdspgres	active
Postgresnotification	active

At the top of the table, there is a 'Delete' button which has been circled in red.

AWS CLI

To delete an Amazon RDS event notification subscription, use the AWS CLI [delete-event-subscription](#) command. Include the following required parameter:

- `--subscription-name`

Example

The following example deletes the subscription `myrdssubscription`.

```
aws rds delete-event-subscription --subscription-name myrdssubscription
```

API

To delete an Amazon RDS event notification subscription, use the RDS API [DeleteEventSubscription](#) command. Include the following required parameter:

- `SubscriptionName`

Creating a rule that triggers on an Amazon RDS event

Using Amazon CloudWatch Events and Amazon EventBridge, you can automate AWS services and respond to system events such as application availability issues or resource changes.

Topics

- [Creating rules to send Amazon RDS events to CloudWatch Events \(p. 664\)](#)
- [Tutorial: Log DB instance state changes using Amazon EventBridge \(p. 665\)](#)

Creating rules to send Amazon RDS events to CloudWatch Events

You can write simple rules to indicate which Amazon RDS events interest you and which automated actions to take when an event matches a rule. You can set a variety of targets, such as an AWS Lambda function or an Amazon SNS topic, which receive events in JSON format. For example, you can configure Amazon RDS to send events to CloudWatch Events or Amazon EventBridge whenever a DB instance is created or deleted. For more information, see the [Amazon CloudWatch Events User Guide](#) and the [Amazon EventBridge User Guide](#).

To create a rule that triggers on an RDS event:

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. Under **Events** in the navigation pane, choose **Rules**.
3. Choose **Create rule**.
4. For **Event Source**, do the following:
 - a. Choose **Event Pattern**.
 - b. For **Service Name**, choose **Relational Database Service (RDS)**.
 - c. For **Event Type**, choose the type of Amazon RDS resource that triggers the event. For example, if a DB instance triggers the event, choose **RDS DB Instance Event**.
5. For **Targets**, choose **Add Target** and choose the AWS service that is to act when an event of the selected type is detected.
6. In the other fields in this section, enter information specific to this target type, if any is needed.
7. For many target types, CloudWatch Events needs permissions to send events to the target. In these cases, CloudWatch Events can create the IAM role needed for your event to run:
 - To create an IAM role automatically, choose **Create a new role for this specific resource**.
 - To use an IAM role that you created before, choose **Use existing role**.
8. Optionally, repeat steps 5-7 to add another target for this rule.
9. Choose **Configure details**. For **Rule definition**, type a name and description for the rule.

The rule name must be unique within this Region.

10. Choose **Create rule**.

For more information, see [Creating a CloudWatch Events Rule That Triggers on an Event](#) in the *Amazon CloudWatch User Guide*.

Tutorial: Log DB instance state changes using Amazon EventBridge

In this tutorial, you create an AWS Lambda function that logs the state changes for an Amazon RDS instance. You then create a rule that runs the function whenever there is a state change of an existing RDS DB instance. The tutorial assumes that you have a small running test instance that you can shut down temporarily.

Important

Don't perform this tutorial on a running production DB instance.

Topics

- [Step 1: Create an AWS Lambda function \(p. 665\)](#)
- [Step 2: Create a rule \(p. 666\)](#)
- [Step 3: Test the rule \(p. 666\)](#)

Step 1: Create an AWS Lambda function

Create a Lambda function to log the state change events. You specify this function when you create your rule.

To create a Lambda function

1. Open the AWS Lambda console at <https://console.aws.amazon.com/lambda/>.
2. If you're new to Lambda, you see a welcome page. Choose **Get Started Now**. Otherwise, choose **Create function**.
3. Choose **Author from scratch**.
4. On the **Create function** page, do the following:
 - a. Enter a name and description for the Lambda function. For example, name the function **RDSInstanceStateChange**.
 - b. In **Runtime**, select **Node.js 16x**.
 - c. For **Architecture**, choose **x86_64**.
 - d. For **Execution role**, do either of the following:
 - Choose **Create a new role with basic Lambda permissions**.
 - For **Existing role**, choose **Use an existing role**. Choose the role that you want to use.
 - e. Choose **Create function**.
5. On the **RDSInstanceStateChange** page, do the following:
 - a. In **Code source**, select **index.js**.
 - b. In the **index.js** pane, delete the existing code.
 - c. Enter the following code:

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('Received event:', JSON.stringify(event));
};
```

- d. Choose **Deploy**.

Step 2: Create a rule

Create a rule to run your Lambda function whenever you launch an Amazon RDS instance.

To create the EventBridge rule

1. Open the Amazon EventBridge console at <https://console.aws.amazon.com/events/>.
2. In the navigation pane, choose **Rules**.
3. Choose **Create rule**.
4. Enter a name and description for the rule. For example, enter **RDSInstanceStateChangeRule**.
5. Choose **Rule with an event pattern**, and then choose **Next**.
6. For **Event source**, choose **AWS events or EventBridge partner events**.
7. Scroll down to the **Event pattern** section.
8. For **Event source**, choose **AWS services**.
9. For **AWS service**, choose **Relational Database Service (RDS)**.
10. For **Event type**, choose **RDS DB Instance Event**.
11. Leave the default event pattern. Then choose **Next**.
12. For **Target types**, choose **AWS service**.
13. For **Select a target**, choose **Lambda function**.
14. For **Function**, choose the Lambda function that you created. Then choose **Next**.
15. In **Configure tags**, choose **Next**.
16. Review the steps in your rule. Then choose **Create rule**.

Step 3: Test the rule

To test your rule, shut down an RDS DB instance. After waiting a few minutes for the instance to shut down, verify that your Lambda function was invoked.

To test your rule by stopping a DB instance

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Stop an RDS DB instance.
3. Open the Amazon EventBridge console at <https://console.aws.amazon.com/events/>.
4. In the navigation pane, choose **Rules**, choose the name of the rule that you created.
5. In **Rule details**, choose **Metrics for the rule**.

You are redirected to the Amazon CloudWatch console.
6. In **All metrics**, choose the name of the rule that you created.

The graph should indicate that the rule was invoked.
7. In the navigation pane, choose **Log groups**.
8. Choose the name of the log group for your Lambda function (`/aws/lambda/function-name`).
9. Choose the name of the log stream to view the data provided by the function for the instance that you launched. You should see a received event similar to the following:

```
{  
  "version": "0",  
  "id": "12a345b6-78c9-01d2-34e5-123f4ghi5j6k",  
  "detail-type": "RDS DB Instance Event",  
  "source": "aws.rds",  
  "account": "111111111111",  
  "time": "2021-03-19T19:34:09Z",  
  "region": "us-east-1",  
  "resources": ["arn:aws:rds:us-east-1:111111111111:db:mydb"]}
```

```
"region": "us-east-1",
"resources": [
    "arn:aws:rds:us-east-1:111111111111:db:testdb"
],
"detail": {
    "EventCategories": [
        "notification"
    ],
    "SourceType": "DB_INSTANCE",
    "SourceArn": "arn:aws:rds:us-east-1:111111111111:db:testdb",
    "Date": "2021-03-19T19:34:09.293Z",
    "Message": "DB instance stopped",
    "SourceIdentifier": "testdb",
    "EventID": "RDS-EVENT-0087"
}
}
```

For more examples of RDS events in JSON format, see [Overview of events for Amazon RDS \(p. 646\)](#).

10. (Optional) When you're finished, you can open the Amazon RDS console and start the instance that you stopped.

Amazon RDS event categories and event messages

Amazon RDS generates a significant number of events in categories that you can subscribe to using the Amazon RDS Console, AWS CLI, or the API.

Topics

- [DB cluster events \(p. 668\)](#)
- [DB instance events \(p. 669\)](#)
- [DB parameter group events \(p. 676\)](#)
- [DB security group events \(p. 676\)](#)
- [DB snapshot events \(p. 677\)](#)
- [DB cluster snapshot events \(p. 678\)](#)
- [RDS Proxy events \(p. 678\)](#)
- [Custom engine version events \(p. 679\)](#)
- [Message attributes \(p. 679\)](#)

DB cluster events

The following table shows the event category and a list of events when a DB cluster is the source type.

For more information about Multi-AZ DB cluster deployments, see [Multi-AZ DB cluster deployments \(p. 127\)](#)

Category	RDS event ID	Description
creation	RDS-EVENT-0170	DB cluster created.
failover	RDS-EVENT-0069	A failover for the DB cluster has failed.
failover	RDS-EVENT-0070	A failover for the DB cluster has restarted.
failover	RDS-EVENT-0071	A failover for the DB cluster has finished.
failover	RDS-EVENT-0072	A failover for the DB cluster has begun within the same Availability Zone.
failover	RDS-EVENT-0073	A failover for the DB cluster has begun across Availability Zones.
global failover	RDS-EVENT-0181	The failover of the global database has started. The process can be delayed because other operations are running on the DB cluster.
global failover	RDS-EVENT-0182	The old primary instance in the global database isn't accepting writes. All volumes are synchronized.
global failover	RDS-EVENT-0183	A replication lag is occurring during the synchronization phase of the global database failover.
global failover	RDS-EVENT-0184	The volume topology of the global database is reestablished with the new primary volume.
global failover	RDS-EVENT-0185	The global database failover is finished on the primary DB cluster. Replicas might take long to come online after the failover completes.

Category	RDS event ID	Description
global failover	RDS-EVENT-0186	The global database failover is canceled.
global failover	RDS-EVENT-0187	The global failover to the DB cluster failed.

DB instance events

The following table shows the event category and a list of events when a DB instance is the source type.

Category	RDS event ID	Description
availability	RDS-EVENT-0006	The DB instance restarted.
availability	RDS-EVENT-0004	DB instance shutdown.
availability	RDS-EVENT-0022	An error has occurred while restarting MySQL.
availability	RDS-EVENT-0221	The DB instance has reached the storage-full threshold, and the database has been shut down. You can increase the allocated storage to address this issue.
availability	RDS-EVENT-0222	Free storage capacity for DB instance [instance name] is low at [percentage]% of the allocated storage (allocated storage: [value], free storage: [value]). The database will be shut down to prevent corruption if free storage is lower than [value]. You can increase the allocated storage to address this issue.
backup	RDS-EVENT-0001	Backing up the DB instance.
backup	RDS-EVENT-0002	Finished DB Instance backup.
backup	RDS-EVENT-0086	RDS was unable to associate the option group with the database instance. Confirm that the option group is supported on your DB instance class and configuration. For more information see Working with option groups (p. 273) .
configuration change	RDS-EVENT-0009	The DB instance has been added to a security group.
configuration change	RDS-EVENT-0024	The DB instance is being converted to a Multi-AZ DB instance.
configuration change	RDS-EVENT-0030	The DB instance is being converted to a Single-AZ DB instance.
configuration change	RDS-EVENT-0012	Applying modification to database instance class.
configuration change	RDS-EVENT-0018	The current storage settings for this DB instance are being changed.
configuration change	RDS-EVENT-0011	A parameter group for this DB instance has changed.

Category	RDS event ID	Description
configuration change	RDS-EVENT-0092	A parameter group for this DB instance has finished updating.
configuration change	RDS-EVENT-0028	Automatic backups for this DB instance have been disabled.
configuration change	RDS-EVENT-0032	Automatic backups for this DB instance have been enabled.
configuration change	RDS-EVENT-0033	There are [count] users that match the master user name. Users not tied to a specific host have been reset.
configuration change	RDS-EVENT-0025	The DB instance has been converted to a Multi-AZ DB instance.
configuration change	RDS-EVENT-0029	The DB instance has been converted to a Single-AZ DB instance.
configuration change	RDS-EVENT-0014	The DB instance class for this DB instance has changed.
configuration change	RDS-EVENT-0017	The storage settings for this DB instance have changed.
configuration change	RDS-EVENT-0010	The DB instance has been removed from a security group.
configuration change	RDS-EVENT-0016	The master password for the DB instance has been reset.
configuration change	RDS-EVENT-0067	An attempt to reset the master password for the DB instance has failed.
configuration change	RDS-EVENT-0078	The Enhanced Monitoring configuration has been changed.
configuration change	RDS-EVENT-0217	Applying autoscaling-initiated modification to allocated storage.
configuration change	RDS-EVENT-0218	Finished applying autoscaling-initiated modification to allocated storage.
creation	RDS-EVENT-0005	DB instance created.
deletion	RDS-EVENT-0003	The DB instance has been deleted.
failover	RDS-EVENT-0013	A Multi-AZ failover that resulted in the promotion of a standby instance has started.
failover	RDS-EVENT-0015	A Multi-AZ failover that resulted in the promotion of a standby instance is complete. It may take several minutes for the DNS to transfer to the new primary DB instance.
failover	RDS-EVENT-0034	Amazon RDS is not attempting a requested failover because a failover recently occurred on the DB instance.

Category	RDS event ID	Description
failover	RDS-EVENT-0049	A Multi-AZ failover has completed.
failover	RDS-EVENT-0050	A Multi-AZ activation has started after a successful instance recovery.
failover	RDS-EVENT-0051	A Multi-AZ activation is complete. Your database should be accessible now.
failover	RDS-EVENT-0065	The instance has recovered from a partial failover.
failure	RDS-EVENT-0031	The DB instance has failed due to an incompatible configuration or an underlying storage issue. Begin a point-in-time-restore for the DB instance.
failure	RDS-EVENT-0035	The DB instance has invalid parameters. For example, if the DB instance could not start because a memory-related parameter is set too high for this instance class, the customer action would be to modify the memory parameter and reboot the DB instance.
failure	RDS-EVENT-0036	The DB instance is in an incompatible network. Some of the specified subnet IDs are invalid or do not exist.
failure	RDS-EVENT-0058	Error while creating Statspack user account PERFSTAT. Drop the account before you add the Statspack option.
failure	RDS-EVENT-0079	Enhanced Monitoring cannot be enabled without the enhanced monitoring IAM role. For information on creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS enhanced monitoring (p. 602) .
failure	RDS-EVENT-0080	Enhanced Monitoring was disabled due to an error making the configuration change. It is likely that the enhanced monitoring IAM role is configured incorrectly. For information on creating the enhanced monitoring IAM role, see To create an IAM role for Amazon RDS enhanced monitoring (p. 602) .
failure	RDS-EVENT-0081	The IAM role that you use to access your Amazon S3 bucket for SQL Server native backup and restore is configured incorrectly. For more information, see Setting up for native backup and restore (p. 1101) .
failure	RDS-EVENT-0165	The RDS Custom DB instance is outside the support perimeter.
failure	RDS-EVENT-0188	Amazon RDS was unable to upgrade a MySQL DB instance from version 5.7 to version 8.0 because of incompatibilities related to the data dictionary. The DB instance was rolled back to MySQL version 5.7. For more information, see Rollback after failure to upgrade from MySQL 5.7 to 8.0 (p. 1347) .
failure	RDS-EVENT-0219	The DB instance is in an invalid state. No actions are necessary. Autoscaling will retry later.

Category	RDS event ID	Description
failure	RDS-EVENT-0220	The DB instance is in the cooling-off period for a previous scale storage operation. We are optimizing your instance. This takes at least six hours. No actions are necessary. Autoscaling will retry after the cooling-off period.
failure	RDS-EVENT-0223	Storage autoscaling is unable to scale the storage for the reason: [reason].
failure	RDS-EVENT-0224	Storage autoscaling has triggered a pending scale storage task that would reach the maximum storage threshold. Increase the maximum storage threshold.
failure	RDS-EVENT-0237	The DB instance has a storage type that's currently unavailable in the Availability Zone. Autoscaling will retry later.
failure	RDS-EVENT-0254	The storage for your AWS account has exceeded the allowed storage quota. Increase the quota to let the autoscaling operation proceed.
low storage	RDS-EVENT-0007	The allocated storage for the DB instance has been consumed. To resolve this issue, allocate additional storage for the DB instance. For more information, see the RDS FAQ . You can monitor the storage space for a DB instance using the Free Storage Space metric.
low storage	RDS-EVENT-0089	The DB instance has consumed more than 90% of its allocated storage. You can monitor the storage space for a DB instance using the Free Storage Space metric.
low storage	RDS-EVENT-0227	The Aurora storage subsystem is running low on space.
maintenance	RDS-EVENT-0026	Offline maintenance of the DB instance is taking place. The DB instance is currently unavailable.
maintenance	RDS-EVENT-0027	Offline maintenance of the DB instance is complete. The DB instance is now available.
maintenance	RDS-EVENT-0047	The DB instance was patched.
maintenance	RDS-EVENT-0155	The DB instance has a DB engine minor version upgrade required.
maintenance, notification	RDS-EVENT-0191	An Oracle time zone file update is available. If you update your Oracle engine, Amazon RDS generates this event if you haven't chosen a time zone file upgrade and the database doesn't use the latest DST time zone file available on the instance. For more information, see Oracle time zone file autoupgrade (p. 1746) .

Category	RDS event ID	Description
maintenance, notification	RDS-EVENT-0192	<p>The upgrade of your Oracle time zone file has begun.</p> <p>For more information, see Oracle time zone file autoupgrade (p. 1746).</p>
maintenance, notification	RDS-EVENT-0193	<p>Your Oracle DB instance is using latest time zone file version, and either of the following is true:</p> <ul style="list-style-type: none"> • You recently added the TIMEZONE_FILE_AUTOUPGRADE option. • Your Oracle DB engine is being upgraded. <p>For more information, see Oracle time zone file autoupgrade (p. 1746).</p>
maintenance, notification	RDS-EVENT-0194	<p>The upgrade of your Oracle time zone file has completed.</p> <p>For more information, see Oracle time zone file autoupgrade (p. 1746).</p>
maintenance, failure	RDS-EVENT-0195	<p>The upgrade of the time zone file failed.</p> <p>For more information, see Oracle time zone file autoupgrade (p. 1746).</p>
notification	RDS-EVENT-0044	Operator-issued notification. For more information, see the event message.
notification	RDS-EVENT-0048	Patching of the DB instance has been delayed.
notification	RDS-EVENT-0054	The MySQL storage engine you are using is not InnoDB, which is the recommended MySQL storage engine for Amazon RDS. For information about MySQL storage engines, see Supported storage engines for RDS for MySQL (p. 1312) .
notification	RDS-EVENT-0055	<p>The number of tables you have for your DB instance exceeds the recommended best practices for Amazon RDS. Reduce the number of tables on your DB instance.</p> <p>For information about recommended best practices, see Amazon RDS basic operational guidelines (p. 216).</p>
notification	RDS-EVENT-0056	<p>The number of databases you have for your DB instance exceeds the recommended best practices for Amazon RDS. Reduce the number of databases on your DB instance.</p> <p>For information about recommended best practices, see Amazon RDS basic operational guidelines (p. 216).</p>
notification	RDS-EVENT-0064	The TDE key has been rotated. For information about recommended best practices, see Amazon RDS basic operational guidelines (p. 216) .

Category	RDS event ID	Description
notification	RDS-EVENT-0084	You attempted to convert a DB instance to Multi-AZ, but it contains in-memory file groups that are not supported for Multi-AZ. For more information, see Multi-AZ deployments for Amazon RDS for Microsoft SQL Server (p. 1129) .
notification	RDS-EVENT-0087	The DB instance has been stopped.
notification	RDS-EVENT-0088	The DB instance has been started.
notification	RDS-EVENT-0154	The DB instance is being started due to it exceeding the maximum allowed time being stopped.
notification	RDS-EVENT-0157	RDS can't modify the DB instance class because the target instance class can't support the number of databases that exist on the source DB instance. The error message appears as: "The instance has <i>N</i> databases, but after conversion it would only support <i>N</i> ". For more information, see Limitations for Microsoft SQL Server DB instances (p. 1060) .
notification	RDS-EVENT-0158	DB instance is in a state that can't be upgraded.
notification	RDS-EVENT-0167	The RDS Custom support perimeter configuration has changed.
notification	RDS-EVENT-0189	The gp2 burst balance credits for the RDS database instance are low. To resolve this issue, reduce IOPS usage or modify your storage settings to enable higher performance. For more information, see I/O credits and burst performance in the Amazon Elastic Compute Cloud User Guide .
notification	RDS-EVENT-0225	Storage size [value] GB is approaching the maximum storage threshold [value] GB. This event is invoked when storage reaches 80% of the maximum storage threshold. To avoid the event, increase the maximum storage threshold.
notification	RDS-EVENT-0231	Your DB instance's storage modification encountered an internal error. The modification request is pending and will be retried later.

Category	RDS event ID	Description
read replica	RDS-EVENT-0045	<p>An error has occurred in the read replication process. For more information, see the event message.</p> <p>In addition, see the troubleshooting section for read replicas for your DB engine.</p> <ul style="list-style-type: none"> • Troubleshooting a MariaDB read replica problem (p. 1033) • Troubleshooting a SQL Server read replica problem (p. 1128) • Troubleshooting a MySQL read replica problem (p. 1399) • Troubleshooting RDS for Oracle replicas (p. 1644)
read replica	RDS-EVENT-0046	The read replica has resumed replication. This message appears when you first create a read replica, or as a monitoring message confirming that replication is functioning properly. If this message follows an RDS-EVENT-0045 notification, then replication has resumed following an error or after replication was stopped.
read replica	RDS-EVENT-0057	Replication on the read replica was terminated.
read replica	RDS-EVENT-0062	Replication on the read replica was manually stopped.
read replica	RDS-EVENT-0063	Replication on the read replica was reset.
read replica	RDS-EVENT-0202	Read replica creation failed.
recovery	RDS-EVENT-0020	Recovery of the DB instance has started. Recovery time will vary with the amount of data to be recovered.
recovery	RDS-EVENT-0021	Recovery of the DB instance is complete.
recovery	RDS-EVENT-0023	A manual backup has been requested but Amazon RDS is currently in the process of creating a DB snapshot. Submit the request again after Amazon RDS has completed the DB snapshot.
recovery	RDS-EVENT-0052	Recovery of the Multi-AZ instance has started. Recovery time will vary with the amount of data to be recovered.
recovery	RDS-EVENT-0053	Recovery of the Multi-AZ instance is complete.
recovery	RDS-EVENT-0066	The SQL Server DB instance is re-establishing its mirror. Performance will be degraded until the mirror is reestablished. A database was found with non-FULL recovery model. The recovery model was changed back to FULL and mirroring recovery was started. (<dbname>: <recovery model found>[,...])"
recovery	RDS-EVENT-0166	The RDS Custom DB instance is inside the support perimeter.

Category	RDS event ID	Description
restoration	RDS-EVENT-0019	The DB instance has been restored from a point-in-time backup.
restoration	RDS-EVENT-0043	Restored from snapshot [snapshot_name]. The DB instance has been restored from a DB snapshot.
security	RDS-EVENT-0068	RDS is decrypting the CloudHSM partition password to make updates to the instance. For more information see Oracle Database Transparent Data Encryption (TDE) with AWS CloudHSM in the AWS CloudHSM User Guide .
security patching	RDS-EVENT-0230	A system update is available for your DB instance. For information about applying updates, see Maintaining a DB instance (p. 350) .

DB parameter group events

The following table shows the event category and a list of events when a DB parameter group is the source type.

Category	RDS event ID	Description
configuration change	RDS-EVENT-0011	Updated to use DBParameterGroup <i>name</i> .
configuration change	RDS-EVENT-0092	Finished updating DB parameter group.

DB security group events

The following table shows the event category and a list of events when a DB security group is the source type.

Note

DB security groups are resources for EC2-Classic. EC2-Classic was retired on August 15, 2022. If you haven't migrated from EC2-Classic to a VPC, we recommend that you migrate as soon as possible. For more information, see [Migrate from EC2-Classic to a VPC](#) in the [Amazon EC2 User Guide](#) and the blog [EC2-Classic Networking is Retiring – Here's How to Prepare](#).

Category	RDS event ID	Description
configuration change	RDS-EVENT-0038	The security group has been modified.
failure	RDS-EVENT-0039	The security group owned by [user] does not exist. Authorization for the security group has been revoked.

DB snapshot events

The following table shows the event category and a list of events when a DB snapshot is the source type.

Category	RDS event ID	Description
creation	RDS-EVENT-0040	A manual DB snapshot is being created.
creation	RDS-EVENT-0042	A manual DB snapshot has been created.
creation	RDS-EVENT-0090	An automated DB snapshot is being created.
creation	RDS-EVENT-0091	An automated DB snapshot has been created.
deletion	RDS-EVENT-0041	A DB snapshot has been deleted.
notification	RDS-EVENT-0059	Started copy of snapshot [DB snapshot name] from region [region name]. Note This is a cross-Region snapshot copy.
notification	RDS-EVENT-0060	Finished copy of snapshot [DB snapshot name] from region [region name] in [time] minutes. Note This is a cross-Region snapshot copy.
notification	RDS-EVENT-0061	Canceled snapshot copy request of [DB snapshot name] from region [region name]. Note This is a cross-Region snapshot copy.
notification	RDS-EVENT-0159	The DB snapshot export task failed.
notification	RDS-EVENT-0160	The DB snapshot export task was canceled.
notification	RDS-EVENT-0161	The DB snapshot export task completed.
notification	RDS-EVENT-0196	Started copy of snapshot [DB snapshot name] in region [region name]. Note This is a local snapshot copy.
notification	RDS-EVENT-0197	Finished copy of snapshot [DB snapshot name] in region [region name]. Note This is a local snapshot copy.
notification	RDS-EVENT-0190	Canceled snapshot copy request of [DB snapshot name] in region [region name]. Note This is a local snapshot copy.
restoration	RDS-EVENT-0043	Restored from snapshot [snapshot_name]. A DB instance is being restored from a DB snapshot.

DB cluster snapshot events

The following table shows the event category and a list of events when a DB cluster snapshot is the source type.

Category	RDS event ID	Description
backup	RDS-EVENT-0074	Creation of a manual DB cluster snapshot has started.
backup	RDS-EVENT-0075	A manual DB cluster snapshot has been created.
backup	RDS-EVENT-0168	Creating automated cluster snapshot.
backup	RDS-EVENT-0169	Automated cluster snapshot created.
notification	RDS-EVENT-0172	Renamed DB cluster from [old DB cluster name] to [new DB cluster name].

RDS Proxy events

The following table shows the event category and a list of events when an RDS Proxy is the source type.

Category	RDS event ID	Description
configuration change	RDS-EVENT-0204	RDS modified the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0207	RDS modified the endpoint of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0213	RDS detected the addition of the DB instance and automatically added it to the target group of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0214	RDS detected the deletion of the DB instance and automatically removed it from the target group of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0215	RDS detected the deletion of the DB cluster and automatically removed it from the target group of the DB proxy (RDS Proxy).
creation	RDS-EVENT-0203	RDS created the DB proxy (RDS Proxy).
creation	RDS-EVENT-0206	RDS created the endpoint for the DB proxy (RDS Proxy).
deletion	RDS-EVENT-0205	RDS deleted the DB proxy (RDS Proxy).
deletion	RDS-EVENT-0208	RDS deleted the endpoint of DB proxy (RDS Proxy).
failure	RDS-EVENT-0243	RDS couldn't provision capacity for the proxy because there aren't enough IP addresses available in your subnets. To fix the issue, make sure that your subnets have the minimum number of unused IP addresses. To determine the recommended number

Category	RDS event ID	Description
		for your instance class, see Planning for IP address capacity (p. 930) .

Custom engine version events

The following table shows the event category and a list of events when a custom engine version is the source type.

Category	Amazon RDS event ID	Description
failure	RDS-EVENT-0198	Creation failed for custom engine version. The message includes details about the failure, such as missing files.

Message attributes

The following table shows the message attribute for RDS events.

Amazon RDS event attribute	Description
Event ID	Identifier for the RDS event message. For example, RDS-EVENT-0006.
Resource	The ARN identifier for the resource emitting the event. For example, arn:aws:rds:ap-southeast-2:123456789012:db:database-1.

Monitoring Amazon RDS log files

Every RDS database engine generates logs that you can access for auditing and troubleshooting. The type of logs depends on your database engine.

You can access database logs using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the Amazon RDS API. You can't view, watch, or download transaction logs.

Topics

- [Viewing and listing database log files \(p. 680\)](#)
- [Downloading a database log file \(p. 681\)](#)
- [Watching a database log file \(p. 682\)](#)
- [Publishing database logs to Amazon CloudWatch Logs \(p. 683\)](#)
- [Reading log file contents using REST \(p. 685\)](#)
- [MariaDB database log files \(p. 687\)](#)
- [Microsoft SQL Server database log files \(p. 696\)](#)
- [MySQL database log files \(p. 700\)](#)
- [Oracle database log files \(p. 709\)](#)
- [RDS for PostgreSQL database log files \(p. 716\)](#)

Viewing and listing database log files

You can view database log files for your Amazon RDS DB engine by using the AWS Management Console. You can list what log files are available for download or monitoring by using the AWS CLI or Amazon RDS API.

Note

If you can't view the list of log files for an existing RDS for Oracle DB instance, reboot the instance to view the list.

Console

To view a database log file

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the **Logs & events** tab.
5. Scroll down to the **Logs** section.
6. (Optional) Enter a search term to filter your results.
7. Choose the log that you want to view, and then choose **View**.

AWS CLI

To list the available database log files for a DB instance, use the AWS CLI `describe-db-log-files` command.

The following example returns a list of log files for a DB instance named `my-db-instance`.

Example

```
aws rds describe-db-log-files --db-instance-identifier my-db-instance
```

RDS API

To list the available database log files for a DB instance, use the Amazon RDS API [DescribeDBLogFiles](#) action.

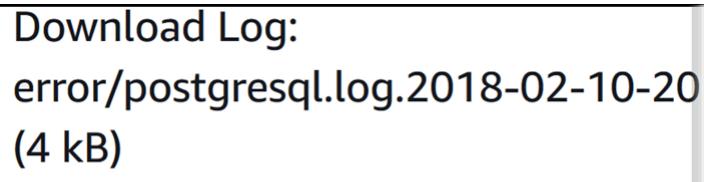
Downloading a database log file

You can use the AWS Management Console, AWS CLI, or API to download a database log file.

Console

To download a database log file

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the **Logs & events** tab.
5. Scroll down to the **Logs** section.
6. In the **Logs** section, choose the button next to the log that you want to download, and then choose **Download**.
7. Open the context (right-click) menu for the link provided, and then choose **Save Link As**. Enter the location where you want the log file to be saved, and then choose **Save**.



AWS CLI

To download a database log file, use the AWS CLI command [download-db-log-file-portion](#). By default, this command downloads only the latest portion of a log file. However, you can download an entire file by specifying the parameter `--starting-token 0`.

The following example shows how to download the entire contents of a log file called *log/ERROR.4* and store it in a local file called *errorlog.txt*.

Example

For Linux, macOS, or Unix:

```
aws rds download-db-log-file-portion \
--db-instance-identifier myexampledb \
--starting-token 0 --output text \
--log-file-name log/ERROR.4 > errorlog.txt
```

For Windows:

```
aws rds download-db-log-file-portion ^
--db-instance-identifier myexampledb ^
--starting-token 0 --output text ^
--log-file-name log/ERROR.4 > errorlog.txt
```

RDS API

To download a database log file, use the Amazon RDS API [DownloadDBLogFilePortion](#) action.

Watching a database log file

Watching a database log file is equivalent to tailing the file on a UNIX or Linux system. You can watch a log file by using the AWS Management Console. RDS refreshes the tail of the log every 5 seconds.

To watch a database log file

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the **Logs & events** tab.

The screenshot shows the AWS RDS console interface. The top navigation bar includes 'RDS', 'Databases', and 'database-1'. On the right, there are 'Modify' and 'Actions' buttons. Below the navigation, the 'Logs & events' tab is highlighted with a red oval. The main area displays a summary table for the database instance 'database-1'. The table includes columns for DB identifier, CPU usage (2.53%), Status (Available), Class (db.m5.large), Role, Current activity (0.00 sessions), Engine (MariaDB), and Region & AZ (us-east-1d). At the bottom of the screen, tabs for 'Connectivity & security', 'Monitoring', 'Logs & events' (which is circled in red), 'Configuration', 'Maintenance & backups', and 'Tags' are visible.

5. In the **Logs** section, choose a log file, and then choose **Watch**.

The screenshot shows the 'Logs' section of the AWS RDS console. The top header says 'Logs (4)' and includes buttons for 'C', 'View', 'Watch', and 'Download'. A search bar labeled 'Filter by db events' is present. The main area lists four log files: 'error/mysql-error-running.log', 'error/mysql-error-running.log.2022-08-02.14', 'error/mysql-error.log', and 'mysqlUpgrade'. Each log entry includes the name, last written timestamp, and size. The second log file, 'error/mysql-error-running.log.2022-08-02.14', is selected and highlighted with a blue border. The 'Watch' button is located in the top right corner of the log list area.

RDS shows the tail of the log, as in the following MySQL example.

Watching Log: error/mysql-error-running.log.2022-08-02.14 (2.9 kB)

text: background:

```
2022-08-02T13:18:12.483484Z 0 [Warning] [MY-011068] [Server] The syntax 'skip_slave_start' is deprecated and will be removed in a future release. Please use skip_replica_start instead.
2022-08-02T13:18:12.483491Z 0 [Warning] [MY-011068] [Server] The syntax 'slave_exec_mode' is deprecated and will be removed in a future release. Please use replica_exec_mode instead.
2022-08-02T13:18:12.483498Z 0 [Warning] [MY-011068] [Server] The syntax 'slave_load_tmpdir' is deprecated and will be removed in a future release. Please use replica_load_tmpdir instead.
2022-08-02T13:18:12.485031Z 0 [Warning] [MY-010101] [Server] Insecure configuration for --secure-file-priv: Location is accessible to all OS users. Consider choosing a different directory.
2022-08-02T13:18:12.485063Z 0 [Warning] [MY-010918] [Server] 'default_authentication_plugin' is deprecated and will be removed in a future release. Please use authentication_policy instead.
2022-08-02T13:18:12.485811Z 0 [System] [MY-010116] [Server] /rdsdbbin/mysql/bin/mysqld (mysqld 8.0.28) starting as process 722
2022-08-02T13:18:12.559455Z 0 [Warning] [MY-010075] [Server] No existing UUID has been found, so we assume that this is the first time that this server has been started. Generating a new UUID: 8f6bd551-1265-11ed-840d-0251cdc2d067.
2022-08-02T13:18:12.580292Z 1 [System] [MY-013576] [InnoDB] InnoDB initialization has started.
2022-08-02T13:18:12.592437Z 1 [Warning] [MY-012191] [InnoDB] Scan path '/rdsdbdata/db/innodb' is ignored because it is a sub-directory of '/rdsdbdata/db/'
2022-08-02T13:18:12.856761Z 1 [System] [MY-013577] [InnoDB] InnoDB initialization has ended.
2022-08-02T13:18:13.126041Z 0 [Warning] [MY-013414] [Server] Server SST certificate doesn't verify: unable to get issuer certificate
2022-08-02T13:18:13.126139Z 0 [System] [MY-013602] [Server] Channel mysql_main configured to support TLS. Encrypted connections are now supported for this channel.
2022-08-02T13:18:13.158424Z 0 [System] [MY-010931] [Server] /rdsdbbin/mysql/bin/mysqld: ready for connections. Version: '8.0.28' socket: '/tmp/mysql.sock' port: 3306 Source distribution.
----- END OF LOG -----
```

Watching error/mysql-error-running.log.2022-08-02.14, updates every 5 seconds.

Publishing database logs to Amazon CloudWatch Logs

In an on-premises database, the database logs reside on the file system. Amazon RDS doesn't provide host access to the database logs on the file system of your DB instance. For this reason, Amazon RDS lets you export database logs to [Amazon CloudWatch Logs](#). With CloudWatch Logs, you can perform real-time analysis of the log data. You can also store the data in highly durable storage and manage the data with the CloudWatch Logs Agent.

Topics

- [Overview of RDS integration with CloudWatch Logs \(p. 683\)](#)
- [Deciding which logs to publish to CloudWatch Logs \(p. 684\)](#)
- [Specifying the logs to publish to CloudWatch Logs \(p. 684\)](#)
- [Searching and filtering your logs in CloudWatch Logs \(p. 684\)](#)

Overview of RDS integration with CloudWatch Logs

In CloudWatch Logs, a *log stream* is a sequence of log events that share the same source. Each separate source of logs in CloudWatch Logs makes up a separate log stream. A *log group* is a group of log streams that share the same retention, monitoring, and access control settings.

Amazon RDS continuously streams your DB instance log records to a log group. For example, you have a log group `/aws/rds/instance/instance_name/log_type` for each type of log that you publish. This log group is in the same AWS Region as the database instance that generates the log.

AWS retains log data published to CloudWatch Logs for an indefinite time period unless you specify a retention period. For more information, see [Change log data retention in CloudWatch Logs](#).

Deciding which logs to publish to CloudWatch Logs

Each RDS database engine supports its own set of logs. To learn about the options for your database engine, review the following topics:

- the section called “Publishing MariaDB logs to Amazon CloudWatch Logs” (p. 689)
- the section called “Publishing MySQL logs to Amazon CloudWatch Logs” (p. 703)
- the section called “Publishing Oracle logs to Amazon CloudWatch Logs” (p. 712)
- the section called “Publishing PostgreSQL logs to Amazon CloudWatch Logs” (p. 721)
- the section called “Publishing SQL Server logs to Amazon CloudWatch Logs” (p. 696)

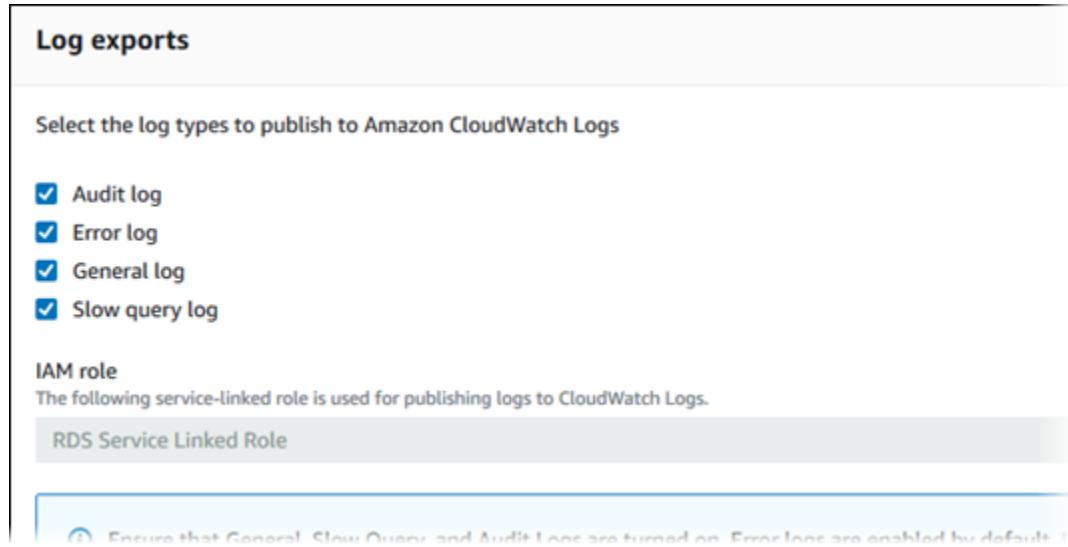
Specifying the logs to publish to CloudWatch Logs

You specify which logs to publish in the console. Make sure that you have a service-linked role in AWS Identity and Access Management (IAM). For more information about service-linked roles, see [Using service-linked roles for Amazon RDS \(p. 2089\)](#).

To specify the logs to publish

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Do either of the following:
 - Choose **Create database**.
 - Choose a database from the list, and then choose **Modify**.
4. In **Logs exports**, choose which logs to publish.

The following example specifies the audit log, error logs, general log, and slow query log.



Searching and filtering your logs in CloudWatch Logs

You can search for log entries that meet a specified criteria using the CloudWatch Logs console. You can access the logs either through the RDS console, which leads you to the CloudWatch Logs console, or from the CloudWatch Logs console directly.

To search your RDS logs using the RDS console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose a DB instance.
4. Choose **Configuration**.
5. Under **Published logs**, choose the database log that you want to view.

To search your RDS logs using the CloudWatch Logs console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Log groups**.
3. In the filter box, enter **/aws/rds**.
4. For **Log Groups**, choose the name of the log group containing the log stream to search.
5. For **Log Streams**, choose the name of the log stream to search.
6. Under **Log events**, enter the filter syntax to use.

For more information, see [Searching and filtering log data](#) in the *Amazon CloudWatch Logs User Guide*. For a blog tutorial explaining how to monitor RDS logs, see [Build proactive database monitoring for Amazon RDS with Amazon CloudWatch Logs, AWS Lambda, and Amazon SNS](#).

Reading log file contents using REST

Amazon RDS provides a REST endpoint that allows access to DB instance log files. This is useful if you need to write an application to stream Amazon RDS log file contents.

The syntax is:

```
GET /v13/downloadCompleteLogFile/DBInstanceIdentifier/LogFileName HTTP/1.1
Content-type: application/json
host: rds.region.amazonaws.com
```

The following parameters are required:

- **DBInstanceIdentifier**—the name of the DB instance that contains the log file you want to download.
- **LogFileName**—the name of the log file to be downloaded.

The response contains the contents of the requested log file, as a stream.

The following example downloads the log file named *log/ERROR.6* for the DB instance named *sample-sql* in the *us-west-2* region.

```
GET /v13/downloadCompleteLogFile/sample-sql/log/ERROR.6 HTTP/1.1
host: rds.us-west-2.amazonaws.com
X-Amz-Security-Token: AQoDYXdzEIH///////////
wEa0AIXLhngC5zp9CyB1R6abwKrXHVR5efnAVN3XvR7IwqKYa1FSn6UyJuEFTft9n0bg1x4QJ+GXV9cpACkETq=
X-Amz-Date: 20140903T233749Z
X-Amz-Algorithm: AWS4-HMAC-SHA256
X-Amz-Credential: AKIADQKE4SARGYLE/20140903/us-west-2/rds/aws4_request
X-Amz-SignedHeaders: host
X-Amz-Content-SHA256: e3b0c44298fc1c229afbf4c8996fb92427ae41e4649b934de495991b7852b855
X-Amz-Expires: 86400
```

X-Amz-Signature: 353a4f14b3f250142d9afc34f9f9948154d46ce7d4ec091d0cdabbcf8b40c558

If you specify a nonexistent DB instance, the response consists of the following error:

- DBInstanceNotFound—*DB Instance Identifier* does not refer to an existing DB instance. (HTTP status code: 404)

MariaDB database log files

You can monitor the MariaDB error log, slow query log, and the general log. The MariaDB error log is generated by default; you can generate the slow query and general logs by setting parameters in your DB parameter group. Amazon RDS rotates all of the MariaDB log files; the intervals for each type are given following.

You can monitor the MariaDB logs directly through the Amazon RDS console, Amazon RDS API, Amazon RDS CLI, or AWS SDKs. You can also access MariaDB logs by directing the logs to a database table in the main database and querying that table. You can use the mysqlbinlog utility to download a binary log.

For more information about viewing, downloading, and watching file-based database logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

Topics

- [Accessing MariaDB error logs \(p. 687\)](#)
- [Accessing the MariaDB slow query and general logs \(p. 687\)](#)
- [Publishing MariaDB logs to Amazon CloudWatch Logs \(p. 689\)](#)
- [Log file size \(p. 691\)](#)
- [Managing table-based MariaDB logs \(p. 691\)](#)
- [Binary logging format \(p. 692\)](#)
- [Accessing MariaDB binary logs \(p. 693\)](#)
- [Binary log annotation \(p. 694\)](#)

Accessing MariaDB error logs

The MariaDB error log is written to the <host-name>.err file. You can view this file by using the Amazon RDS console, You can also retrieve the log using the Amazon RDS API, Amazon RDS CLI, or AWS SDKs. The <host-name>.err file is flushed every 5 minutes, and its contents are appended to mysql-error-running.log. The mysql-error-running.log file is then rotated every hour and the hourly files generated during the last 24 hours are retained. Each log file has the hour it was generated (in UTC) appended to its name. The log files also have a timestamp that helps you determine when the log entries were written.

MariaDB writes to the error log only on startup, shutdown, and when it encounters errors. A DB instance can go hours or days without new entries being written to the error log. If you see no recent entries, it's because the server did not encounter an error that resulted in a log entry.

Accessing the MariaDB slow query and general logs

You can write the MariaDB slow query log and general log to a file or database table by setting parameters in your DB parameter group. For information about creating and modifying a DB parameter group, see [Working with parameter groups \(p. 289\)](#). You must set these parameters before you can view the slow query log or general log in the Amazon RDS console or by using the Amazon RDS API, AWS CLI, or AWS SDKs.

You can control MariaDB logging by using the parameters in this list:

- `slow_query_log`: To create the slow query log, set to 1. The default is 0.
- `general_log`: To create the general log, set to 1. The default is 0.
- `long_query_time`: To prevent fast-running queries from being logged in the slow query log, specify a value for the shortest query run time to be logged, in seconds. The default is 10 seconds; the

minimum is 0. If `log_output = FILE`, you can specify a floating point value that goes to microsecond resolution. If `log_output = TABLE`, you must specify an integer value with second resolution. Only queries whose run time exceeds the `long_query_time` value are logged. For example, setting `long_query_time` to 0.1 prevents any query that runs for less than 100 milliseconds from being logged.

- `log_queries_not_using_indexes`: To log all queries that do not use an index to the slow query log, set this parameter to 1. The default is 0. Queries that do not use an index are logged even if their run time is less than the value of the `long_query_time` parameter.
- `log_output option`: You can specify one of the following options for the `log_output` parameter:
 - **TABLE** (default)– Write general queries to the `mysql.general_log` table, and slow queries to the `mysql.slow_log` table.
 - **FILE**– Write both general and slow query logs to the file system. Log files are rotated hourly.
 - **NONE**– Disable logging.

When logging is enabled, Amazon RDS rotates table logs or deletes log files at regular intervals. This measure is a precaution to reduce the possibility of a large log file either blocking database use or affecting performance. FILE and TABLE logging approach rotation and deletion as follows:

- When FILE logging is enabled, log files are examined every hour and log files older than 24 hours are deleted. In some cases, the remaining combined log file size after the deletion might exceed the threshold of 2 percent of a DB instance's allocated space. In these cases, the largest log files are deleted until the log file size no longer exceeds the threshold.
- When TABLE logging is enabled, in some cases log tables are rotated every 24 hours. This rotation occurs if the space used by the table logs is more than 20 percent of the allocated storage space. It also occurs if the size of all logs combined is greater than 10 GB. If the amount of space used for a DB instance is greater than 90 percent of the DB instance's allocated storage space, the thresholds for log rotation are reduced. Log tables are then rotated if the space used by the table logs is more than 10 percent of the allocated storage space. They're also rotated if the size of all logs combined is greater than 5 GB.

When log tables are rotated, the current log table is copied to a backup log table and the entries in the current log table are removed. If the backup log table already exists, then it is deleted before the current log table is copied to the backup. You can query the backup log table if needed. The backup log table for the `mysql.general_log` table is named `mysql.general_log_backup`. The backup log table for the `mysql.slow_log` table is named `mysql.slow_log_backup`.

You can rotate the `mysql.general_log` table by calling the `mysql.rds_rotate_general_log` procedure. You can rotate the `mysql.slow_log` table by calling the `mysql.rds_rotate_slow_log` procedure.

Table logs are rotated during a database version upgrade.

Amazon RDS records both TABLE and FILE log rotation in an Amazon RDS event and sends you a notification.

To work with the logs from the Amazon RDS console, Amazon RDS API, Amazon RDS CLI, or AWS SDKs, set the `log_output` parameter to FILE. Like the MariaDB error log, these log files are rotated hourly. The log files that were generated during the previous 24 hours are retained.

For more information about the slow query and general logs, go to the following topics in the MariaDB documentation:

- [Slow query log](#)
- [General query log](#)

Publishing MariaDB logs to Amazon CloudWatch Logs

You can configure your MariaDB DB instance to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage.

Amazon RDS publishes each MariaDB database log as a separate database stream in the log group. For example, suppose that you configure the export function to include the slow query log. Then slow query data is stored in a slow query log stream in the /aws/rds/instance/*my_instance*/slowquery log group.

The error log is enabled by default. The following table summarizes the requirements for the other MariaDB logs.

Log	Requirement
Audit log	The DB instance must use a custom option group with the MARIADB_AUDIT_PLUGIN option.
General log	The DB instance must use a custom parameter group with the parameter setting general_log = 1 to enable the general log.
Slow query log	The DB instance must use a custom parameter group with the parameter setting slow_query_log = 1 to enable the slow query log.
Log output	The DB instance must use a custom parameter group with the parameter setting log_output = FILE to write logs to the file system and publish them to CloudWatch Logs.

Console

To publish MariaDB logs to CloudWatch Logs from the console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**.
4. In the **Log exports** section, choose the logs that you want to start publishing to CloudWatch Logs.
5. Choose **Continue**, and then choose **Modify DB Instance** on the summary page.

AWS CLI

You can publish a MariaDB logs with the AWS CLI. You can call the `modify-db-instance` command with the following parameters:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

Note

A change to the `--cloudwatch-logs-export-configuration` option is always applied to the DB instance immediately. Therefore, the `--apply-immediately` and `--no-apply-immediately` options have no effect.

You can also publish MariaDB logs by calling the following AWS CLI commands:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Run one of these AWS CLI commands with the following options:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Other options might be required depending on the AWS CLI command you run.

Example

The following example modifies an existing MariaDB DB instance to publish log files to CloudWatch Logs. The `--cloudwatch-logs-export-configuration` value is a JSON object. The key for this object is `EnableLogTypes`, and its value is an array of strings with any combination of `audit`, `error`, `general`, and `slowquery`.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": \
    ["audit","error","general","slowquery"]}'
```

For Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": \
    ["audit","error","general","slowquery"]}'
```

Example

The following command creates a MariaDB DB instance and publishes log files to CloudWatch Logs. The `--enable-cloudwatch-logs-exports` value is a JSON array of strings. The strings can be any combination of `audit`, `error`, `general`, and `slowquery`.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '[{"audit","error","general","slowquery"}' \
```

```
--db-instance-class db.m4.large \
--engine mariadb
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--enable-cloudwatch-logs-exports '[{"audit","error","general","slowquery"}]' ^
--db-instance-class db.m4.large ^
--engine mariadb
```

RDS API

You can publish MariaDB logs with the RDS API. You can call the [ModifyDBInstance](#) operation with the following parameters:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

Note

A change to the `CloudwatchLogsExportConfiguration` parameter is always applied to the DB instance immediately. Therefore, the `ApplyImmediately` parameter has no effect.

You can also publish MariaDB logs by calling the following RDS API operations:

- [CreateDBInstance](#)
- [RestoreDBInstanceFromDBSnapshot](#)
- [RestoreDBInstanceFromS3](#)
- [RestoreDBInstanceToPointInTime](#)

Run one of these RDS API operations with the following parameters:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

Other parameters might be required depending on the AWS CLI command you run.

Log file size

The MariaDB slow query log, error log, and the general log file sizes are constrained to no more than 2 percent of the allocated storage space for a DB instance. To maintain this threshold, logs are automatically rotated every hour and log files older than 24 hours are removed. If the combined log file size exceeds the threshold after removing old log files, then the largest log files are deleted until the log file size no longer exceeds the threshold.

Managing table-based MariaDB logs

You can direct the general and slow query logs to tables on the DB instance. To do so, create a DB parameter group and set the `log_output` server parameter to TABLE. General queries are then logged

to the `mysql.general_log` table, and slow queries are logged to the `mysql.slow_log` table. You can query the tables to access the log information. Enabling this logging increases the amount of data written to the database, which can degrade performance.

Both the general log and the slow query logs are disabled by default. In order to enable logging to tables, you must also set the `general_log` and `slow_query_log` server parameters to 1.

Log tables keep growing until the respective logging activities are turned off by resetting the appropriate parameter to 0. A large amount of data often accumulates over time, which can use up a considerable percentage of your allocated storage space. Amazon RDS does not allow you to truncate the log tables, but you can move their contents. Rotating a table saves its contents to a backup table and then creates a new empty log table. You can manually rotate the log tables with the following command line procedures, where the command prompt is indicated by PROMPT>:

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

To completely remove the old data and reclaim the disk space, call the appropriate procedure twice in succession.

Binary logging format

MariaDB on Amazon RDS supports the *row-based*, *statement-based*, and *mixed* binary logging formats. The default binary logging format is *mixed*. For details on the different MariaDB binary log formats, see [Binary log formats](#) in the MariaDB documentation.

If you plan to use replication, the binary logging format is important. This is because it determines the record of data changes that is recorded in the source and sent to the replication targets. For information about the advantages and disadvantages of different binary logging formats for replication, see [Advantages and disadvantages of statement-based and row-based replication](#) in the MySQL documentation.

Important

Setting the binary logging format to row-based can result in very large binary log files. Large binary log files reduce the amount of storage available for a DB instance. They also can increase the amount of time to perform a restore operation of a DB instance.

Statement-based replication can cause inconsistencies between the source DB instance and a read replica. For more information, see [Unsafe statements for statement-based replication](#) in the MariaDB documentation.

To set the MariaDB binary logging format

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group that is used by the DB instance that you want to modify.

You can't modify a default parameter group. If the DB instance is using a default parameter group, create a new parameter group and associate it with the DB instance.

For more information on DB parameter groups, see [Working with parameter groups \(p. 289\)](#).

4. For **Parameter group actions**, choose **Edit**.
5. Set the `binlog_format` parameter to the binary logging format of your choice (**ROW**, **STATEMENT**, or **MIXED**).
6. Choose **Save changes** to save the updates to the DB parameter group.

Accessing MariaDB binary logs

You can use the `mysqlbinlog` utility to download binary logs in text format from MariaDB DB instances. The binary log is downloaded to your local computer. For more information about using the `mysqlbinlog` utility, go to [Using mysqlbinlog](#) in the MariaDB documentation.

To run the `mysqlbinlog` utility against an Amazon RDS instance, use the following options:

- Specify the `--read-from-remote-server` option.
- `--host`: Specify the DNS name from the endpoint of the instance.
- `--port`: Specify the port used by the instance.
- `--user`: Specify a MariaDB user that has been granted the replication slave permission.
- `--password`: Specify the password for the user, or omit a password value so the utility prompts you for a password.
- `--result-file`: Specify the local file that receives the output.
- Specify the names of one or more binary log files. To get a list of the available logs, use the SQL command `SHOW BINARY LOGS`.

For more information about `mysqlbinlog` options, go to [mysqlbinlog options](#) in the MariaDB documentation.

The following is an example:

For Linux, macOS, or Unix:

```
mysqlbinlog \
  --read-from-remote-server \
  --host=mariadbinstance1.1234abcd.region.rds.amazonaws.com \
  --port=3306 \
  --user ReplUser \
  --password <password> \
  --result-file=/tmp/binlog.txt
```

For Windows:

```
mysqlbinlog ^
  --read-from-remote-server ^
  --host=mariadbinstance1.1234abcd.region.rds.amazonaws.com ^
  --port=3306 ^
  --user ReplUser ^
  --password <password> ^
  --result-file=/tmp/binlog.txt
```

Amazon RDS normally purges a binary log as soon as possible. However, the binary log must still be available on the instance to be accessed by `mysqlbinlog`. To specify the number of hours for RDS to retain binary logs, use the `mysql.rds_set_configuration` stored procedure. Specify a period with enough time for you to download the logs. After you set the retention period, monitor storage usage for the DB instance to ensure that the retained binary logs don't take up too much storage.

The following example sets the retention period to 1 day.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

To display the current setting, use the `mysql.rds_show_configuration` stored procedure.

```
call mysql.rds_show_configuration;
```

Binary log annotation

In a MariaDB DB instance, you can use the Annotate_rows event to annotate a row event with a copy of the SQL query that caused the row event. This approach provides similar functionality to enabling the binlog_rows_query_log_events parameter on an RDS for MySQL DB instance.

You can enable binary log annotations globally by creating a custom parameter group and setting the binlog_annotate_row_events parameter to 1. You can also enable annotations at the session level, by calling SET SESSION binlog_annotate_row_events = 1. Use the replicate_annotate_row_events to replicate binary log annotations to the replica instance if binary logging is enabled on it. No special privileges are required to use these settings.

The following is an example of a row-based transaction in MariaDB. The use of row-based logging is triggered by setting the transaction isolation level to read-committed.

```
CREATE DATABASE IF NOT EXISTS test;
USE test;
CREATE TABLE square(x INT PRIMARY KEY, y INT NOT NULL) ENGINE = InnoDB;
SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED;
BEGIN
INSERT INTO square(x, y) VALUES(5, 5 * 5);
COMMIT;
```

Without annotations, the binary log entries for the transaction look like the following:

```
BEGIN
/*!*/
# at 1163
# at 1209
#150922 7:55:57 server id 1855786460  end_log_pos 1209      Table_map: `test`.`square`
mapped to number 76
#150922 7:55:57 server id 1855786460  end_log_pos 1247      Write_rows: table id 76
flags: STMT_END_F
### INSERT INTO `test`.`square`
### SET
###   @1=5
###   @2=25
# at 1247
#150922 7:56:01 server id 1855786460  end_log_pos 1274      Xid = 62
COMMIT/*!*/;
```

The following statement enables session-level annotations for this same transaction, and disables them after committing the transaction:

```
CREATE DATABASE IF NOT EXISTS test;
USE test;
CREATE TABLE square(x INT PRIMARY KEY, y INT NOT NULL) ENGINE = InnoDB;
SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED;
SET SESSION binlog_annotate_row_events = 1;
BEGIN;
INSERT INTO square(x, y) VALUES(5, 5 * 5);
COMMIT;
SET SESSION binlog_annotate_row_events = 0;
```

With annotations, the binary log entries for the transaction look like the following:

```
BEGIN
```

```
/*!*/;
# at 423
# at 483
# at 529
#150922 8:04:24 server id 1855786460  end_log_pos 483  Annotate_rows:
#Q> INSERT INTO square(x, y) VALUES(5, 5 * 5)
#150922 8:04:24 server id 1855786460  end_log_pos 529  Table_map: `test`.`square` mapped
to number 76
#150922 8:04:24 server id 1855786460  end_log_pos 567  Write_rows: table id 76 flags:
STMT_END_F
### INSERT INTO `test`.`square`
### SET
###   @1=5
###   @2=25
# at 567
#150922 8:04:26 server id 1855786460  end_log_pos 594  Xid = 88
COMMIT/*!*/;
```

Microsoft SQL Server database log files

You can access Microsoft SQL Server error logs, agent logs, trace files, and dump files by using the Amazon RDS console, AWS CLI, or RDS API. For more information about viewing, downloading, and watching file-based database logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

Topics

- [Retention schedule \(p. 696\)](#)
- [Viewing the SQL Server error log by using the rds_read_error_log procedure \(p. 696\)](#)
- [Publishing SQL Server logs to Amazon CloudWatch Logs \(p. 696\)](#)

Retention schedule

Log files are rotated each day and whenever your DB instance is restarted. The following is the retention schedule for Microsoft SQL Server logs on Amazon RDS.

Log type	Retention schedule
Error logs	A maximum of 30 error logs are retained. Amazon RDS might delete error logs older than 7 days.
Agent logs	A maximum of 10 agent logs are retained. Amazon RDS might delete agent logs older than 7 days.
Trace files	Trace files are retained according to the trace file retention period of your DB instance. The default trace file retention period is 7 days. To modify the trace file retention period for your DB instance, see Setting the retention period for trace and dump files (p. 1309) .
Dump files	Dump files are retained according to the dump file retention period of your DB instance. The default dump file retention period is 7 days. To modify the dump file retention period for your DB instance, see Setting the retention period for trace and dump files (p. 1309) .

Viewing the SQL Server error log by using the rds_read_error_log procedure

You can use the Amazon RDS stored procedure `rds_read_error_log` to view error logs and agent logs. For more information, see [Viewing error and agent logs \(p. 1308\)](#).

Publishing SQL Server logs to Amazon CloudWatch Logs

With Amazon RDS for SQL Server, you can publish error and agent log events directly to Amazon CloudWatch Logs. Analyze the log data with CloudWatch Logs, then use CloudWatch to create alarms and view metrics.

With CloudWatch Logs, you can do the following:

- Store logs in highly durable storage space with a retention period that you define.
- Search and filter log data.
- Share log data between accounts.

- Export logs to Amazon S3.
- Stream data to Amazon OpenSearch Service.
- Process log data in real time with Amazon Kinesis Data Streams. For more information, see [Working with Amazon CloudWatch Logs](#) in the *Amazon Kinesis Data Analytics for SQL Applications Developer Guide*.

Amazon RDS publishes each SQL Server database log as a separate database stream in the log group. For example, if you publish error logs, error data is stored in an error log stream in the `/aws/rds/instance/my_instance/error` log group.

For Multi-AZ DB instances, Amazon RDS publishes the database log as two separate streams in the log group. For example, if you publish the error logs, the error data is stored in the error log streams `/aws/rds/instance/my_instance.node1/error` and `/aws/rds/instance/my_instance.node2/error` respectively. The log streams don't change during a failover and the error log stream of each node can contain error logs from primary or secondary instance.

Note

Publishing SQL Server logs to CloudWatch Logs isn't enabled by default. Publishing trace and dump files isn't supported. Publishing SQL Server logs to CloudWatch Logs is supported in all regions, except for Asia Pacific (Hong Kong).

Console

To publish SQL Server DB logs to CloudWatch Logs from the AWS Management Console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**.
4. In the **Log exports** section, choose the logs that you want to start publishing to CloudWatch Logs.
You can choose **Agent log**, **Error log**, or both.
5. Choose **Continue**, and then choose **Modify DB Instance** on the summary page.

AWS CLI

To publish SQL Server logs, you can use the `modify-db-instance` command with the following parameters:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

Note

A change to the `--cloudwatch-logs-export-configuration` option is always applied to the DB instance immediately. Therefore, the `--apply-immediately` and `--no-apply-immediately` options have no effect.

You can also publish SQL Server logs using the following commands:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Example

The following example creates an SQL Server DB instance with CloudWatch Logs publishing enabled. The --enable-cloudwatch-logs-exports value is a JSON array of strings that can include error, agent, or both.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '[{"error", "agent"}]' \
    --db-instance-class db.m4.large \
    --engine sqlserver-se
```

For Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports "[\"error\", \"agent\"]" ^
    --db-instance-class db.m4.large ^
    --engine sqlserver-se
```

Note

When using the Windows command prompt, you must escape double quotes ("") in JSON code by prefixing them with a backslash (\).

Example

The following example modifies an existing SQL Server DB instance to publish log files to CloudWatch Logs. The --cloudwatch-logs-export-configuration value is a JSON object. The key for this object is EnableLogTypes, and its value is an array of strings that can include error, agent, or both.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["error", "agent"]}'
```

For Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"EnableLogTypes\": [\"error\", \"agent\"]}"
```

Note

When using the Windows command prompt, you must escape double quotes ("") in JSON code by prefixing them with a backslash (\).

Example

The following example modifies an existing SQL Server DB instance to disable publishing agent log files to CloudWatch Logs. The --cloudwatch-logs-export-configuration value is a JSON object. The key for this object is DisableLogTypes, and its value is an array of strings that can include error, agent, or both.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
```

```
--db-instance-identifier mydbinstance \
--cloudwatch-logs-export-configuration '{"DisableLogTypes":["agent"]}'
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--cloudwatch-logs-export-configuration "{\"DisableLogTypes\": [\"agent\"]}"
```

Note

When using the Windows command prompt, you must escape double quotes ("") in JSON code by prefixing them with a backslash (\).

MySQL database log files

You can monitor the MySQL logs directly through the Amazon RDS console, Amazon RDS API, AWS CLI, or AWS SDKs. You can also access MySQL logs by directing the logs to a database table in the main database and querying that table. You can use the `mysqlbinlog` utility to download a binary log.

For more information about viewing, downloading, and watching file-based database logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

Topics

- [Overview of RDS for MySQL database logs \(p. 700\)](#)
- [Publishing MySQL logs to Amazon CloudWatch Logs \(p. 703\)](#)
- [Managing table-based MySQL logs \(p. 705\)](#)
- [Configuring MySQL binary logging \(p. 706\)](#)
- [Accessing MySQL binary logs \(p. 707\)](#)

Overview of RDS for MySQL database logs

You can monitor the following types of RDS for MySQL log files:

- Error log
- Slow query log
- General log
- Audit log

The RDS for MySQL error log is generated by default. You can generate the slow query and general logs by setting parameters in your DB parameter group.

Topics

- [RDS for MySQL error logs \(p. 700\)](#)
- [RDS for MySQL slow query and general logs \(p. 701\)](#)
- [MySQL audit log \(p. 701\)](#)
- [Log rotation and retention for RDS for MySQL \(p. 701\)](#)
- [Size limits on redo logs \(p. 702\)](#)
- [Size limits on BLOBs written to the redo log \(p. 702\)](#)

RDS for MySQL error logs

RDS for MySQL writes errors in the `mysql-error.log` file. Each log file has the hour it was generated (in UTC) appended to its name. The log files also have a timestamp that helps you determine when the log entries were written.

RDS for MySQL writes to the error log only on startup, shutdown, and when it encounters errors. A DB instance can go hours or days without new entries being written to the error log. If you see no recent entries, it's because the server didn't encounter an error that would result in a log entry.

By design, the error logs are filtered so that only unexpected events such as errors are shown. However, the error logs also contain some additional database information, for example query progress, which isn't shown. Therefore, even without any actual errors the size of the error logs might increase because of ongoing database activities.

RDS for MySQL writes `mysql-error.log` to disk every 5 minutes. It appends the contents of the log to `mysql-error-running.log`.

RDS for MySQL rotates the `mysql-error-running.log` file every hour. It retains the logs generated during the last two weeks.

Note

The log retention period is different between Amazon RDS and Aurora.

RDS for MySQL slow query and general logs

You can write the RDS for MySQL slow query log and the general log to a file or a database table. To do so, set parameters in your DB parameter group. For information about creating and modifying a DB parameter group, see [Working with parameter groups \(p. 289\)](#). You must set these parameters before you can view the slow query log or general log in the Amazon RDS console or by using the Amazon RDS API, Amazon RDS CLI, or AWS SDKs.

You can control RDS for MySQL logging by using the parameters in this list:

- `slow_query_log`: To create the slow query log, set to 1. The default is 0.
- `general_log`: To create the general log, set to 1. The default is 0.
- `long_query_time`: To prevent fast-running queries from being logged in the slow query log, specify a value for the shortest query runtime to be logged, in seconds. The default is 10 seconds; the minimum is 0. If `log_output = FILE`, you can specify a floating point value that goes to microsecond resolution. If `log_output = TABLE`, you must specify an integer value with second resolution. Only queries whose runtime exceeds the `long_query_time` value are logged. For example, setting `long_query_time` to 0.1 prevents any query that runs for less than 100 milliseconds from being logged.
- `log_queries_not_using_indexes`: To log all queries that do not use an index to the slow query log, set to 1. Queries that don't use an index are logged even if their runtime is less than the value of the `long_query_time` parameter. The default is 0.
- `log_output option`: You can specify one of the following options for the `log_output` parameter.
 - **TABLE** (default) – Write general queries to the `mysql.general_log` table, and slow queries to the `mysql.slow_log` table.
 - **FILE** – Write both general and slow query logs to the file system.
 - **NONE** – Disable logging.

For more information about the slow query and general logs, go to the following topics in the MySQL documentation:

- [The slow query log](#)
- [The general query log](#)

MySQL audit log

To access the audit log, the DB instance must use a custom option group with the `MARIADB_AUDIT_PLUGIN` option. For more information, see [MariaDB Audit Plugin support \(p. 1417\)](#).

Log rotation and retention for RDS for MySQL

When logging is enabled, Amazon RDS rotates table logs or deletes log files at regular intervals. This measure is a precaution to reduce the possibility of a large log file either blocking database use or affecting performance. RDS for MySQL handles rotation and deletion as follows:

- The MySQL slow query log, error log, and the general log file sizes are constrained to no more than 2 percent of the allocated storage space for a DB instance. To maintain this threshold, logs are automatically rotated every hour. MySQL removes log files more than two weeks old. If the combined log file size exceeds the threshold after removing old log files, then the oldest log files are deleted until the log file size no longer exceeds the threshold.
- When FILE logging is enabled, log files are examined every hour and log files more than two weeks old are deleted. In some cases, the remaining combined log file size after the deletion might exceed the threshold of 2 percent of a DB instance's allocated space. In these cases, the oldest log files are deleted until the log file size no longer exceeds the threshold.
- When TABLE logging is enabled, in some cases log tables are rotated every 24 hours. This rotation occurs if the space used by the table logs is more than 20 percent of the allocated storage space. It also occurs if the size of all logs combined is greater than 10 GB. If the amount of space used for a DB instance is greater than 90 percent of the DB instance's allocated storage space, then the thresholds for log rotation are reduced. Log tables are then rotated if the space used by the table logs is more than 10 percent of the allocated storage space. They're also rotated if the size of all logs combined is greater than 5 GB. You can subscribe to the [low_free_storage](#) event to be notified when log tables are rotated to free up space. For more information, see [Working with Amazon RDS event notification \(p. 650\)](#).

When log tables are rotated, the current log table is first copied to a backup log table. Then the entries in the current log table are removed. If the backup log table already exists, then it is deleted before the current log table is copied to the backup. You can query the backup log table if needed. The backup log table for the `mysql.general_log` table is named `mysql.general_log_backup`. The backup log table for the `mysql.slow_log` table is named `mysql.slow_log_backup`.

You can rotate the `mysql.general_log` table by calling the `mysql.rds_rotate_general_log` procedure. You can rotate the `mysql.slow_log` table by calling the `mysql.rds_rotate_slow_log` procedure.

Table logs are rotated during a database version upgrade.

To work with the logs from the Amazon RDS console, Amazon RDS API, Amazon RDS CLI, or AWS SDKs, set the `log_output` parameter to `FILE`. Like the MySQL error log, these log files are rotated hourly. The log files that were generated during the previous two weeks are retained. Note that the retention period is different between Amazon RDS and Aurora.

Size limits on redo logs

For RDS for MySQL version 8.0.28 and lower, the `innodb_log_file_size` parameter determines the size of redo logs. The default value of this parameter is 256 MB. For information about limitations related to this limit, see [Size limits on BLOBs written to the redo log \(p. 702\)](#). For more information on how redo log size is calculated for these versions of MySQL, see `innodb_log_file_size` in the MySQL documentation.

For RDS for MySQL version 8.0.30 and higher, the `innodb_redo_log_capacity` parameter is used instead of the `innodb_log_file_size` parameter. The default value of the `innodb_redo_log_capacity` parameter is 2 GB. For more information, see [Changes in MySQL 8.0.30 in the MySQL documentation](#).

Size limits on BLOBs written to the redo log

For RDS for MySQL version 8.0.28 and lower, there is a size limit on BLOBs written to the redo log. To account for this limit, check the `innodb_log_file_size` parameter for your MySQL DB instance. Make sure that it is 10 times larger than the largest BLOB data size found in your tables plus the length of other variable length fields (VARCHAR, VARBINARY, TEXT) in these tables. For information about how to set parameter values, see [Working with parameter groups \(p. 289\)](#). For information about the redo log BLOB size limit, see [Changes in MySQL 5.6.20](#) in the MySQL documentation.

For RDS for MySQL version 8.0.30 and higher, the `innodb_redo_log_capacity` parameter is used instead of the `innodb_log_file_size` parameter. The size limit doesn't apply to the `innodb_redo_log_capacity` parameter. For more information, see [Size limits on redo logs \(p. 702\)](#).

Publishing MySQL logs to Amazon CloudWatch Logs

You can configure your MySQL DB instance to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can perform real-time analysis of the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage.

Amazon RDS publishes each MySQL database log as a separate database stream in the log group. For example, if you configure the export function to include the slow query log, slow query data is stored in a slow query log stream in the `/aws/rds/instance/my_instance/slowquery` log group.

The error log is enabled by default. The following table summarizes the requirements for the other MySQL logs.

Log	Requirement
Audit log	The DB instance must use a custom option group with the <code>MARIADB_AUDIT_PLUGIN</code> option.
General log	The DB instance must use a custom parameter group with the parameter setting <code>general_log = 1</code> to enable the general log.
Slow query log	The DB instance must use a custom parameter group with the parameter setting <code>slow_query_log = 1</code> to enable the slow query log.
Log output	The DB instance must use a custom parameter group with the parameter setting <code>log_output = FILE</code> to write logs to the file system and publish them to CloudWatch Logs.

Console

To publish MySQL logs to CloudWatch Logs using the console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**.
4. In the **Log exports** section, choose the logs that you want to start publishing to CloudWatch Logs.
5. Choose **Continue**, and then choose **Modify DB Instance** on the summary page.

AWS CLI

You can publish MySQL logs with the AWS CLI. You can call the `modify-db-instance` command with the following parameters:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

Note

A change to the `--cloudwatch-logs-export-configuration` option is always applied to the DB instance immediately. Therefore, the `--apply-immediately` and `--no-apply-immediately` options have no effect.

You can also publish MySQL logs by calling the following AWS CLI commands:

- [create-db-instance](#)
- [restore-db-instance-from-db-snapshot](#)
- [restore-db-instance-from-s3](#)
- [restore-db-instance-to-point-in-time](#)

Run one of these AWS CLI commands with the following options:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Other options might be required depending on the AWS CLI command you run.

Example

The following example modifies an existing MySQL DB instance to publish log files to CloudWatch Logs. The `--cloudwatch-logs-export-configuration` value is a JSON object. The key for this object is `EnableLogTypes`, and its value is an array of strings with any combination of `audit`, `error`, `general`, and `slowquery`.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": \
    ["audit","error","general","slowquery"]}'
```

For Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": \
    ["audit","error","general","slowquery"]}'
```

Example

The following example creates a MySQL DB instance and publishes log files to CloudWatch Logs. The `--enable-cloudwatch-logs-exports` value is a JSON array of strings. The strings can be any combination of `audit`, `error`, `general`, and `slowquery`.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '[{"audit","error","general","slowquery"}' \
```

```
--db-instance-class db.m4.large \
--engine MySQL
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--enable-cloudwatch-logs-exports '[{"audit","error","general","slowquery"}]' ^
--db-instance-class db.m4.large ^
--engine MySQL
```

RDS API

You can publish MySQL logs with the RDS API. You can call the [ModifyDBInstance](#) action with the following parameters:

- [DBInstanceIdentifier](#)
- [CloudwatchLogsExportConfiguration](#)

Note

A change to the [CloudwatchLogsExportConfiguration](#) parameter is always applied to the DB instance immediately. Therefore, the [ApplyImmediately](#) parameter has no effect.

You can also publish MySQL logs by calling the following RDS API operations:

- [CreateDBInstance](#)
- [RestoreDBInstanceFromDBSnapshot](#)
- [RestoreDBInstanceFromS3](#)
- [RestoreDBInstanceToPointInTime](#)

Run one of these RDS API operations with the following parameters:

- [DBInstanceIdentifier](#)
- [EnableCloudwatchLogsExports](#)
- [Engine](#)
- [DBInstanceClass](#)

Other parameters might be required depending on the AWS CLI command you run.

Managing table-based MySQL logs

You can direct the general and slow query logs to tables on the DB instance by creating a DB parameter group and setting the `log_output` server parameter to TABLE. General queries are then logged to the `mysql.general_log` table, and slow queries are logged to the `mysql.slow_log` table. You can query the tables to access the log information. Enabling this logging increases the amount of data written to the database, which can degrade performance.

Both the general log and the slow query logs are disabled by default. In order to enable logging to tables, you must also set the `general_log` and `slow_query_log` server parameters to 1.

Log tables keep growing until the respective logging activities are turned off by resetting the appropriate parameter to 0. A large amount of data often accumulates over time, which can use up a considerable

percentage of your allocated storage space. Amazon RDS doesn't allow you to truncate the log tables, but you can move their contents. Rotating a table saves its contents to a backup table and then creates a new empty log table. You can manually rotate the log tables with the following command line procedures, where the command prompt is indicated by PROMPT>:

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

To completely remove the old data and reclaim the disk space, call the appropriate procedure twice in succession.

Configuring MySQL binary logging

The *binary log* is a set of log files that contain information about data modifications made to an MySQL server instance. The binary log contains information such as the following:

- Events that describe database changes such as table creation or row modifications
- Information about the duration of each statement that updated data
- Events for statements that could have updated data but didn't

The binary log records statements that are sent during replication. It is also required for some recovery operations. For more information, see [The Binary Log](#) and [Binary Log Overview](#) in the MySQL documentation.

The automated backups feature determines whether binary logging is turned on or off for MySQL. You have the following options:

Turn binary logging on

Set the backup retention period to a positive nonzero value.

Turn binary logging off

Set the backup retention period to zero.

For more information, see [Enabling automated backups \(p. 429\)](#).

MySQL on Amazon RDS supports the *row-based*, *statement-based*, and *mixed* binary logging formats. We recommend mixed unless you need a specific binlog format. For details on the different MySQL binary log formats, see [Binary logging formats](#) in the MySQL documentation.

If you plan to use replication, the binary logging format is important because it determines the record of data changes that is recorded in the source and sent to the replication targets. For information about the advantages and disadvantages of different binary logging formats for replication, see [Advantages and disadvantages of statement-based and row-based replication](#) in the MySQL documentation.

Important

Setting the binary logging format to row-based can result in very large binary log files. Large binary log files reduce the amount of storage available for a DB instance and can increase the amount of time to perform a restore operation of a DB instance.

Statement-based replication can cause inconsistencies between the source DB instance and a read replica. For more information, see [Determination of safe and unsafe statements in binary logging](#) in the MySQL documentation.

To set the MySQL binary logging format

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group used by the DB instance you want to modify.

You can't modify a default parameter group. If the DB instance is using a default parameter group, create a new parameter group and associate it with the DB instance.

For more information on parameter groups, see [Working with parameter groups \(p. 289\)](#).

4. From **Parameter group actions**, choose **Edit**.
5. Set the `binlog_format` parameter to the binary logging format of your choice (**ROW**, **STATEMENT**, or **MIXED**). You can also use the value **OFF** to turn off binary logging.
6. Choose **Save changes** to save the updates to the DB parameter group.

After you perform these steps, you must reboot the DB instance for your changes to apply. For more information, see [Rebooting a DB instance \(p. 366\)](#).

Important

Changing a DB parameter group affects all DB instances that use that parameter group. If you want to specify different binary logging formats for different MySQL DB instances in an AWS Region, the DB instances must use different DB parameter groups. These parameter groups identify different logging formats. Assign the appropriate DB parameter group to the each DB instance.

Accessing MySQL binary logs

You can use the `mysqlbinlog` utility to download or stream binary logs from RDS for MySQL DB instances. The binary log is downloaded to your local computer, where you can perform actions such as replaying the log using the `mysql` utility. For more information about using the `mysqlbinlog` utility, go to [Using mysqlbinlog to back up binary log files](#).

To run the `mysqlbinlog` utility against an Amazon RDS instance, use the following options:

- Specify the `--read-from-remote-server` option.
- `--host`: Specify the DNS name from the endpoint of the instance.
- `--port`: Specify the port used by the instance.
- `--user`: Specify a MySQL user that has been granted the replication slave permission.
- `--password`: Specify the password for the user, or omit a password value so that the utility prompts you for a password.
- To have the file downloaded in binary format, specify the `--raw` option.
- `--result-file`: Specify the local file to receive the raw output.
- Specify the names of one or more binary log files. To get a list of the available logs, use the SQL command `SHOW BINARY LOGS`.
- To stream the binary log files, specify the `--stop-never` option.

For more information about `mysqlbinlog` options, go to [mysqlbinlog - utility for processing binary log files](#).

For example, see the following.

For Linux, macOS, or Unix:

```
mysqlbinlog \
  --read-from-remote-server \
  --host=MySQL56Instance1.cg034hpkmmt.region.rds.amazonaws.com \
  --port=3306 \
```

```
--user ReplUser \
--password \
--raw \
--result-file=/tmp/ \
binlog.00098
```

For Windows:

```
mysqlbinlog ^
--read-from-remote-server ^
--host=MySQL56Instance1.cg034hpkmmt.region.rds.amazonaws.com ^
--port=3306 ^
--user ReplUser ^
--password ^
--raw ^
--result-file=/tmp/ ^
binlog.00098
```

Amazon RDS normally purges a binary log as soon as possible, but the binary log must still be available on the instance to be accessed by mysqlbinlog. To specify the number of hours for RDS to retain binary logs, use the `mysql.rds_set_configuration` stored procedure and specify a period with enough time for you to download the logs. After you set the retention period, monitor storage usage for the DB instance to ensure that the retained binary logs don't take up too much storage.

The following example sets the retention period to 1 day.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

To display the current setting, use the `mysql.rds_show_configuration` stored procedure.

```
call mysql.rds_show_configuration;
```

Oracle database log files

You can access Oracle alert logs, audit files, and trace files by using the Amazon RDS console or API. For more information about viewing, downloading, and watching file-based database logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

The Oracle audit files provided are the standard Oracle auditing files. Amazon RDS supports the Oracle fine-grained auditing (FGA) feature. However, log access doesn't provide access to FGA events that are stored in the SYS.FGA_LOG\$ table and that are accessible through the DBA_FGA_AUDIT_TRAIL view.

The [DescribeDBLogFiles](#) API operation that lists the Oracle log files that are available for a DB instance ignores the MaxRecords parameter and returns up to 1,000 records. The call returns LastWritten as a POSIX date in milliseconds.

Topics

- [Retention schedule \(p. 709\)](#)
- [Working with Oracle trace files \(p. 709\)](#)
- [Publishing Oracle logs to Amazon CloudWatch Logs \(p. 712\)](#)
- [Previous methods for accessing alert logs and listener logs \(p. 715\)](#)

Retention schedule

The Oracle database engine might rotate log files if they get very large. To retain audit or trace files, download them. If you store the files locally, you reduce your Amazon RDS storage costs and make more space available for your data.

The following table shows the retention schedule for Oracle alert logs, audit files, and trace files on Amazon RDS.

Log type	Retention schedule
Alert logs	The text alert log is rotated daily with 30-day retention managed by Amazon RDS. The XML alert log is retained for at least seven days. You can access this log by using the ALERTLOG view.
Audit files	The default retention period for audit files is seven days. Amazon RDS might delete audit files older than seven days.
Trace files	The default retention period for trace files is seven days. Amazon RDS might delete trace files older than seven days.
Listener logs	The default retention period for the listener logs is seven days. Amazon RDS might delete listener logs older than seven days.

Note

Audit files and trace files share the same retention configuration.

Working with Oracle trace files

Following, you can find descriptions of Amazon RDS procedures to create, refresh, access, and delete trace files.

Topics

- [Listing files \(p. 710\)](#)
- [Generating trace files and tracing a session \(p. 710\)](#)
- [Retrieving trace files \(p. 711\)](#)
- [Purging trace files \(p. 711\)](#)

Listing files

You can use either of two procedures to allow access to any file in the background_dump_dest path. The first procedure refreshes a view containing a listing of all files currently in background_dump_dest.

```
EXEC rdsadmin.manage_tracefiles.refresh_tracefile_listing;
```

After the view is refreshed, query the following view to access the results.

```
SELECT * FROM rdsadmin.tracefile_listing;
```

An alternative to the previous process is to use FROM table to stream nonrelational data in a table-like format to list database directory contents.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('BDUMP'));
```

The following query shows the text of a log file.

```
SELECT text FROM
  TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP','alert_dbname.log.date'));
```

On a read replica, get the name of the BDUMP directory by querying V\$DATABASE.DB_UNIQUE_NAME. If the unique name is DATABASE_B, then the BDUMP directory is BDUMP_B. The following example queries the BDUMP name on a replica and then uses this name to query the contents of alert_DATABASE.log.2020-06-23.

```
SELECT 'BDUMP' || (SELECT regexp_replace(DB_UNIQUE_NAME,'.*(_[A-Z])', '\1') FROM V$DATABASE) AS BDUMP_VARIABLE FROM DUAL;
-----
BDUMP_VARIABLE
-----
BDUMP_B

SELECT TEXT FROM
  table(rdsadmin.rds_file_util.read_text_file('BDUMP_B','alert_DATABASE.log.2020-06-23'));
```

Generating trace files and tracing a session

Because there are no restrictions on ALTER SESSION, many standard methods to generate trace files in Oracle remain available to an Amazon RDS DB instance. The following procedures are provided for trace files that require greater access.

Oracle method	Amazon RDS method
oradebug hanganalyze 3	EXEC rdsadmin.manage_tracefiles.hanganalyze;

Oracle method	Amazon RDS method
oradebug dump systemstate 266	EXEC rdsadmin.manage_tracefiles.dump_systemstate;

You can use many standard methods to trace individual sessions connected to an Oracle DB instance in Amazon RDS. To enable tracing for a session, you can run subprograms in PL/SQL packages supplied by Oracle, such as DBMS_SESSION and DBMS_MONITOR. For more information, see [Enabling tracing for a session](#) in the Oracle documentation.

Retrieving trace files

You can retrieve any trace file in background_dump_dest using a standard SQL query on an Amazon RDS-managed external table. To use this method, you must execute the procedure to set the location for this table to the specific trace file.

For example, you can use the rdsadmin.tracefile_listing view mentioned preceding to list all of the trace files on the system. You can then set the tracefile_table view to point to the intended trace file using the following procedure.

```
EXEC
rdsadmin.manage_tracefiles.set_tracefile_table_location('CUST01_ora_3260_SYSTEMSTATE.trc');
```

The following example creates an external table in the current schema with the location set to the file provided. You can retrieve the contents into a local file using a SQL query.

```
SPPOOL /tmp/tracefile.txt
SELECT * FROM tracefile_table;
SPPOOL OFF;
```

Purging trace files

Trace files can accumulate and consume disk space. Amazon RDS purges trace files by default and log files that are older than seven days. You can view and set the trace file retention period using the show_configuration procedure. You should run the command SET SERVEROUTPUT ON so that you can view the configuration results.

The following example shows the current trace file retention period, and then sets a new trace file retention period.

```
# Show the current tracefile retention
SQL> EXEC rdsadmin.rdsadmin_util.show_configuration;
NAME:tracefile retention
VALUE:10080
DESCRIPTION:tracefile expiration specifies the duration in minutes before tracefiles in
bdbump are automatically deleted.

# Set the tracefile retention to 24 hours:
SQL> EXEC rdsadmin.rdsadmin_util.set_configuration('tracefile retention',1440);
SQL> commit;

#show the new tracefile retention
SQL> EXEC rdsadmin.rdsadmin_util.show_configuration;
NAME:tracefile retention
VALUE:1440
DESCRIPTION:tracefile expiration specifies the duration in minutes before tracefiles in
bdbump are automatically deleted.
```

In addition to the periodic purge process, you can manually remove files from the background_dump_dest. The following example shows how to purge all files older than five minutes.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles(5);
```

You can also purge all files that match a specific pattern (if you do, don't include the file extension, such as .trc). The following example shows how to purge all files that start with SCHPOC1_ora_5935.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles('SCHPOC1_ora_5935');
```

Publishing Oracle logs to Amazon CloudWatch Logs

You can configure your Amazon RDS for Oracle DB instance to publish log data to a log group in Amazon CloudWatch Logs. With CloudWatch Logs, you can analyze the log data, and use CloudWatch to create alarms and view metrics. You can use CloudWatch Logs to store your log records in highly durable storage.

Amazon RDS publishes each Oracle database log as a separate database stream in the log group. For example, if you configure the export function to include the audit log, audit data is stored in an audit log stream in the /aws/rds/instance/my_instance/audit log group. RDS for Oracle supports the following logs:

- Alert log
- Trace log
- Audit log
- Listener log
- Oracle Management Agent log

This Oracle Management Agent log consists of the log groups shown in the following table.

Log name	CloudWatch log group
emctl.log	oemagent-emctl
emdctlj.log	oemagent-emdctlj
gcagent.log	oemagent-gcagent
gcagent_errors.log	oemagent-gcagent-errors
emagent.nohup	oemagent-emagent-nohup
secure.log	oemagent-secure

For more information, see [Locating Management Agent Log and Trace Files](#) in the Oracle documentation.

Console

To publish Oracle DB logs to CloudWatch Logs from the AWS Management Console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**.

4. In the **Log exports** section, choose the logs that you want to start publishing to CloudWatch Logs.
5. Choose **Continue**, and then choose **Modify DB Instance** on the summary page.

AWS CLI

To publish Oracle logs, you can use the `modify-db-instance` command with the following parameters:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

Note

A change to the `--cloudwatch-logs-export-configuration` option is always applied to the DB instance immediately. Therefore, the `--apply-immediately` and `--no-apply-immediately` options have no effect.

You can also publish Oracle logs using the following commands:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Example

The following example creates an Oracle DB instance with CloudWatch Logs publishing enabled. The `--cloudwatch-logs-export-configuration` value is a JSON array of strings. The strings can be any combination of alert, audit, listener, and trace.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration
    '['"trace","audit","alert","listener","oemagent"]' \
    --db-instance-class db.m5.large \
    --allocated-storage 20 \
    --engine oracle-ee \
    --engine-version 12.1.0.2.v18 \
    --license-model bring-your-own-license \
    --master-username myadmin \
    --master-user-password mypassword
```

For Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration trace alert audit listener oemagent ^
    --db-instance-class db.m5.large ^
    --allocated-storage 20 ^
    --engine oracle-ee ^
    --engine-version 12.1.0.2.v18 ^
    --license-model bring-your-own-license ^
    --master-username myadmin ^
    --master-user-password mypassword
```

Example

The following example modifies an existing Oracle DB instance to publish log files to CloudWatch Logs. The --cloudwatch-logs-export-configuration value is a JSON object. The key for this object is EnableLogTypes, and its value is an array of strings with any combination of alert, audit, listener, and trace.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--cloudwatch-logs-export-configuration '{"EnableLogTypes": \
["trace", "alert", "audit", "listener", "oemagent"]}'
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--cloudwatch-logs-export-configuration EnableLogTypes="trace\", \"alert\", \"audit\",
\"listener\", \"oemagent\""
```

Example

The following example modifies an existing Oracle DB instance to disable publishing audit and listener log files to CloudWatch Logs. The --cloudwatch-logs-export-configuration value is a JSON object. The key for this object is DisableLogTypes, and its value is an array of strings with any combination of alert, audit, listener, and trace.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--cloudwatch-logs-export-configuration '{"DisableLogTypes": ["audit", "listener"]}'
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--cloudwatch-logs-export-configuration DisableLogTypes="audit\", \"listener\""
```

RDS API

You can publish Oracle DB logs with the RDS API. You can call the [ModifyDBInstance](#) action with the following parameters:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

Note

A change to the `CloudwatchLogsExportConfiguration` parameter is always applied to the DB instance immediately. Therefore, the `ApplyImmediately` parameter has no effect.

You can also publish Oracle logs by calling the following RDS API operations:

- [CreateDBInstance](#)
- [RestoreDBInstanceFromDBSnapshot](#)

- [RestoreDBInstanceFromS3](#)
- [RestoreDBInstanceToPointInTime](#)

Run one of these RDS API operations with the following parameters:

- DBInstanceIdentifier
- EnableCloudwatchLogsExports
- Engine
- DBInstanceClass

Other parameters might be required depending on the RDS operation that you run.

Previous methods for accessing alert logs and listener logs

You can view the alert log using the Amazon RDS console. You can also use the following SQL statement to access the alert log.

```
SELECT message_text FROM alertlog;
```

The listenerlog view contains entries for Oracle Database version 12.1.0.2 and earlier. To access the listener log for these database versions, use the following query.

```
SELECT message_text FROM listenerlog;
```

For Oracle Database versions 12.2.0.1 and later, access the listener log using Amazon CloudWatch Logs.

Note

Oracle rotates the alert and listener logs when they exceed 10 MB, at which point they are unavailable from Amazon RDS views.

RDS for PostgreSQL database log files

RDS for PostgreSQL logs database activities to the default PostgreSQL log file. For an on-premises PostgreSQL DB instance, these messages are stored locally in `log/postgresql.log`. For an RDS for PostgreSQL DB instance, the log file is available on the Amazon RDS instance. Also, you must use the Amazon RDS Console to view or download its contents. The default logging level captures login failures, fatal server errors, deadlocks, and query failures.

For more information about how you can view, download, and watch file-based database logs, see [Monitoring Amazon RDS log files \(p. 680\)](#). To learn more about PostgreSQL logs, see [Working with Amazon RDS and Aurora PostgreSQL logs: Part 1](#) and [Working with Amazon RDS and Aurora PostgreSQL logs: Part 2](#).

In addition to the standard PostgreSQL logs discussed in this topic, RDS for PostgreSQL also supports the PostgreSQL Audit extension (`pgAudit`). Most regulated industries and government agencies need to maintain an audit log or audit trail of changes made to data to comply with legal requirements. For information about installing and using `pgAudit`, see [Using pgAudit to log database activity \(p. 1951\)](#).

Topics

- [Parameters that affect logging behavior \(p. 716\)](#)
- [Turning on query logging for your RDS for PostgreSQL DB instance \(p. 718\)](#)
- [Publishing PostgreSQL logs to Amazon CloudWatch Logs \(p. 721\)](#)

Parameters that affect logging behavior

You can customize the logging behavior for your RDS for PostgreSQL DB instance by modifying various parameters. In the following table you can find the parameters that affect how long the logs are stored, when to rotate the log, and whether to output the log as a CSV (comma-separated value) format. You can also find the text output sent to `STDERR`, among other settings. To change settings for the parameters that are modifiable, use a custom DB parameter group for your RDS for PostgreSQL instance. For more information, see [Working with DB parameter groups \(p. 291\)](#). As noted in the table, the `log_line_prefix` can't be changed.

Parameter	Default	Description
<code>log_destination</code>	<code>stderr</code>	Sets the output format for the log. The default is <code>stderr</code> but you can also specify comma-separated value (CSV) by adding <code>csvlog</code> to the setting. For more information, see Setting the log destination (stderr, csvlog) (p. 718)
<code>log_filename</code>	<code>postgresql.log.%Y-%m-%d-%H</code>	Specifies the pattern for the log file name. In addition to the default, this parameter supports <code>postgresql.log.%Y-%m-%d</code> for the filename pattern.
<code>log_line_prefix</code>	<code>%t:%r:%u@%d:[%p]:</code>	Defines the prefix for each log line that gets written to <code>stderr</code> , to note the time (<code>%t</code>), remote host (<code>%r</code>), user (<code>%u</code>), database (<code>%d</code>), and process ID (<code>%p</code>). You can't modify this parameter.
<code>log_rotation_age</code>	60	Minutes after which log file is automatically rotated. You can change this value to between 1 and 1440 minutes. For more information, see Setting log file rotation (p. 717) .

Parameter	Default	Description
log_rotation_size	–	The size (kB) at which the log is automatically rotated. By default, this parameter isn't used because logs are rotated based on the log_rotation_age parameter. To learn more, see Setting log file rotation (p. 717) .
rds.log_retention_period	4320	PostgreSQL logs that are older than the specified number of minutes are deleted. The default value of 4320 minutes deletes log files after 3 days. For more information, see Setting the log retention period (p. 717) .

To identify application issues, you can look for query failures, login failures, deadlocks, and fatal server errors in the log. For example, suppose that you converted a legacy application from Oracle to Amazon RDS PostgreSQL, but not all queries converted correctly. These incorrectly formatted queries generate error messages that you can find in the logs to help identify problems. For more information about logging queries, see [Turning on query logging for your RDS for PostgreSQL DB instance \(p. 718\)](#).

In the following topics, you can find information about how to set various parameters that control the basic details for your PostgreSQL logs.

Topics

- [Setting the log retention period \(p. 717\)](#)
- [Setting log file rotation \(p. 717\)](#)
- [Setting the log destination \(stderr, csvlog\) \(p. 718\)](#)
- [Understanding the log_line_prefix parameter \(p. 718\)](#)

Setting the log retention period

The rds.log_retention_period parameter specifies how long your RDS for PostgreSQL DB instance keeps its log files. The default setting is 3 days (4,320 minutes), but you can set this value to anywhere from 1 day (1,440 minutes) to 7 days (10,080 minutes). Be sure that your RDS for PostgreSQL DB instance has sufficient storage to hold the log files for the period of time.

We recommend that you have your logs routinely published to Amazon CloudWatch Logs so that you can view and analyze system data long after the logs have been removed from your RDS for PostgreSQL DB instance. For more information, see [Publishing PostgreSQL logs to Amazon CloudWatch Logs \(p. 721\)](#).

Setting log file rotation

Amazon RDS creates new log files every hour by default. The timing is controlled by the log_rotation_age parameter. This parameter has a default value of 60 (minutes), but you can set it to anywhere from 1 minute to 24 hours (1,440 minutes). When it's time for rotation, a new distinct log file is created. The file is named according to the pattern specified by the log_filename parameter.

Log files can also be rotated according to their size, as specified in the log_rotation_size parameter. This parameter specifies that the log should be rotated when it reaches the specified size (in kilobytes). For an RDS for PostgreSQL DB instance, log_rotation_size is unset, that is, there is no value specified. However, you can set the parameter from 0-2097151 kB (kilobytes).

The log file names are based on the file name pattern specified in the log_filename parameter. The available settings for this parameter are as follows:

- `postgresql.log.%Y-%m-%d` – Default format for the log file name. Includes the year, month, and date in the name of the log file.
- `postgresql.log.%Y-%m-%d-%H` – Includes the hour in the log file name format.

For more information, see [log_rotation_age](#) and [log_rotation_size](#) in the PostgreSQL documentation.

Setting the log destination (`stderr`, `csvlog`)

By default, Amazon RDS PostgreSQL generates logs in standard error (`stderr`) format. This format is the default setting for the `log_destination` parameter. Each message is prefixed using the pattern specified in the `log_line_prefix` parameter. For more information, see [Understanding the log_line_prefix parameter \(p. 718\)](#).

RDS for PostgreSQL can also generate the logs in `csvlog` format. The `csvlog` is useful for analyzing the log data as comma-separated values (CSV) data. For example, suppose that you use the `log_fdw` extension to work with your logs as foreign tables. The foreign table created on `stderr` log files contains a single column with log event data. By adding `csvlog` to the `log_destination` parameter, you get the log file in the CSV format with demarcations for the multiple columns of the foreign table. You can now sort and analyze your logs more easily. To learn how to use the `log_fdw` with `csvlog`, see [Using the log_fdw extension to access the DB log using SQL \(p. 1987\)](#).

If you specify `csvlog` for this parameter, be aware that both `stderr` and `csvlog` files are generated. Be sure to monitor the storage consumed by the logs, taking into account the `rds.log_retention_period` and other settings that affect log storage and turnover. Using `stderr` and `csvlog` more than doubles the storage consumed by the logs.

If you add `csvlog` to `log_destination` and you want to revert to the `stderr` alone, you need to reset the parameter. To do so, open the Amazon RDS Console and then open the custom DB parameter group for your instance. Choose the `log_destination` parameter, choose **Edit parameter**, and then choose **Reset**.

For more information about configuring logging, see [Working with Amazon RDS and Aurora PostgreSQL logs: Part 1](#).

Understanding the `log_line_prefix` parameter

The `stderr` log format prefixes each log message with the details specified by the `log_line_prefix` parameter, as follows.

```
%t:%r:%u@d:[%p]:t
```

You can't change this setting. Each log entry sent to `stderr` includes the following information.

- `%t` – Time of log entry
- `%r` – Remote host address
- `%u@d` – User name @ database name
- `[%p]` – Process ID if available

Turning on query logging for your RDS for PostgreSQL DB instance

You can collect more detailed information about your database activities, including queries, queries waiting for locks, checkpoints, and many other details by setting some of the parameters listed in the following table. This topic focuses on logging queries.

Parameter	Default	Description
log_connections	–	Logs each successful connection.
log_disconnections	–	Logs the end of each session and its duration.
log_checkpoints	1	Logs each checkpoint.
log_lock_waits	–	Logs long lock waits. By default, this parameter isn't set.
log_min_duration_sample	–	(ms) Sets the minimum execution time above which a sample of statements is logged. Sample size is set using the log_statement_sample_rate parameter.
log_min_duration_statement	all	Sets the type of statements logged.
log_statement	–	Sets the type of statements logged. By default, this parameter isn't set, but you can change it to all, ddl, or mod to specify the types of SQL statements that you want logged. If you specify anything other than none for this parameter, you should also take additional steps to prevent the exposure of passwords in the log files. For more information, see Mitigating risk of password exposure when using query logging (p. 721) .
log_statement_sample_rate		The percentage of statements exceeding the time specified in log_min_duration_sample to be logged, expressed as a floating point value between 0.0 and 1.0.
log_statement_stats	–	Writes cumulative performance statistics to the server log.

Using logging to find slow performing queries

You can log SQL statements and queries to help find slow performing queries. You turn on this capability by modifying the settings in the log_statement and log_min_duration parameters as outlined in this section. Before turning on query logging for your RDS for PostgreSQL DB instance, you should be aware of possible password exposure in the logs and how to mitigate the risks. For more information, see [Mitigating risk of password exposure when using query logging \(p. 721\)](#).

Following, you can find reference information about the log_statement and log_min_duration parameters.

log_statement

This parameter specifies the type of SQL statements that should get sent to the log. The default value is none. If you change this parameter to all, ddl, or mod, be sure to apply recommended actions to mitigate the risk of exposing passwords in the logs. For more information, see [Mitigating risk of password exposure when using query logging \(p. 721\)](#).

all

Logs all statements. This setting is recommended for debugging purposes.

ddl

Logs all data definition language (DDL) statements, such as CREATE, ALTER, DROP, and so on.

mod

Logs all DDL statements and data manipulation language (DML) statements, such as INSERT, UPDATE, and DELETE, which modify the data.

none

No SQL statements get logged. We recommend this setting to avoid the risk of exposing passwords in the logs.

log_min_duration_statement

Any SQL statement that runs longer than the number of milliseconds specified by this parameter setting gets logged. By default, this parameter isn't set. Turning on this parameter can help you find unoptimized queries.

-1-2147483647

The number of milliseconds (ms) of runtime over which a statement gets logged.

To set up query logging

These steps assume that your RDS for PostgreSQL DB instance uses a custom DB parameter group.

1. Set the `log_statement` parameter to `all`. The following example shows the information that is written to the `postgresql.log` file with this parameter setting.

```
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: statement: SELECT
  feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: QUERY STATISTICS
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:DETAIL: ! system usage
  stats:
! 0.017355 s user, 0.000000 s system, 0.168593 s elapsed
! [0.025146 s user, 0.000000 s system total]
! 36644 kB max resident size
! 0/8 [0/8] filesystem blocks in/out
! 0/733 [0/1364] page faults/reclaims, 0 [0] swaps
! 0 [0] signals rcvd, 0/0 [0/0] messages rcvd/sent
! 19/0 [27/0] voluntary/involuntary context switches
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: SELECT
  feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:ERROR: syntax error at
  or near "ORDER" at character 1
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: ORDER BY
  s.confidence DESC;
----- END OF LOG -----
```

2. Set the `log_min_duration_statement` parameter. The following example shows the information that is written to the `postgresql.log` file when the parameter is set to 1.

Queries that exceed the duration specified in the `log_min_duration_statement` parameter are logged. The following shows an example. You can view the log file for your RDS for PostgreSQL DB instance in the Amazon RDS Console.

```
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: statement: DROP
table comments;
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: duration: 167.754 ms
2022-10-05 19:08:07 UTC:@:[355]:LOG: checkpoint starting: time
2022-10-05 19:08:08 UTC:@:[355]:LOG: checkpoint complete: wrote 11 buffers (0.0%); 0
WAL file(s) added, 0 removed, 0 recycled; write=1.013 s, sync=0.006 s, total=1.033 s;
sync files=8, longest=0.004 s, average=0.001 s; distance=131028 kB, estimate=131028 kB
----- END OF LOG -----
```

Mitigating risk of password exposure when using query logging

We recommend that you keep `log_statement` set to none to avoid exposing passwords. If you set `log_statement` to all, ddl, or mod, we recommend that you take one or more of the following steps.

- For the client, encrypt sensitive information. For more information, see [Encryption Options](#) in the PostgreSQL documentation. Use the ENCRYPTED (and UNENCRYPTED) options of the CREATE and ALTER statements. For more information, see [CREATE USER](#) in the PostgreSQL documentation.
- For your RDS for PostgreSQL DB instance, set up and use the PostgreSQL Auditing (pgAudit) extension. This extension redacts sensitive information in CREATE and ALTER statements sent to the log. For more information, see [Using pgAudit to log database activity \(p. 1951\)](#).
- Restrict access to the CloudWatch logs.
- Use stronger authentication mechanisms such as IAM.

Publishing PostgreSQL logs to Amazon CloudWatch Logs

To store your PostgreSQL log records in highly durable storage, you can use Amazon CloudWatch Logs. With CloudWatch Logs, you can also perform real-time analysis of log data and use CloudWatch to view metrics and create alarms. For example, if you set `log_statements` to ddl, you can set up an alarm to alert you whenever a DDL statement is executed. You can choose to have your PostgreSQL logs uploaded to CloudWatch Logs during the process of creating your RDS for PostgreSQL DB instance. If you chose not to upload logs at that time, you can later modify your instance to start uploading logs from that point forward. In other words, existing logs aren't uploaded. Only new logs are uploaded as they're created on your modified RDS for PostgreSQL DB instance. When PostgreSQL logs are uploaded to CloudWatch Logs, they're no longer kept in the **Logs** section of the **Logs & events** tab. Instead, to view them you CloudWatch to view your logs.

All currently available RDS for PostgreSQL versions support publishing log files to CloudWatch Logs. For more information, see [Amazon RDS for PostgreSQL updates](#) in the *Amazon RDS for PostgreSQL Release Notes*.

To work with CloudWatch Logs, configure your RDS for PostgreSQL DB instance to publish log data to a log group.

You can publish the following log types to CloudWatch Logs for RDS for PostgreSQL:

- Postgresql log
- Upgrade log

After you complete the configuration, Amazon RDS publishes the log events to log streams within a CloudWatch log group. For example, the PostgreSQL log data is stored within the log group `/aws/rds/instance/my_instance/postgresql`. To view your logs, open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

Console

To publish PostgreSQL logs to CloudWatch Logs using the console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify, and then choose **Modify**.
4. In the **Log exports** section, choose the logs that you want to start publishing to CloudWatch Logs.

The **Log exports** section is available only for PostgreSQL versions that support publishing to CloudWatch Logs.

5. Choose **Continue**, and then choose **Modify DB Instance** on the summary page.

AWS CLI

You can publish PostgreSQL logs with the AWS CLI. You can call the `modify-db-instance` command with the following parameters.

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

Note

A change to the `--cloudwatch-logs-export-configuration` option is always applied to the DB instance immediately. Therefore, the `--apply-immediately` and `--no-apply-immediately` options have no effect.

You can also publish PostgreSQL logs by calling the following CLI commands:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Run one of these CLI commands with the following options:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Other options might be required depending on the CLI command you run.

Example Modify an instance to publish logs to CloudWatch Logs

The following example modifies an existing PostgreSQL DB instance to publish log files to CloudWatch Logs. The `--cloudwatch-logs-export-configuration` value is a JSON object. The key for this object is `EnableLogTypes`, and its value is an array of strings with any combination of `postgresql` and `upgrade`.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes": ["postgresql", "upgrade"]}'
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--cloudwatch-logs-export-configuration '{"EnableLogTypes": ["postgresql", "upgrade"]}'
```

Example Create an instance to publish logs to CloudWatch Logs

The following example creates a PostgreSQL DB instance and publishes log files to CloudWatch Logs. The --enable-cloudwatch-logs-exports value is a JSON array of strings. The strings can be any combination of postgresql and upgrade.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier mydbinstance \
--enable-cloudwatch-logs-exports '['"postgresql", "upgrade"]' \
--db-instance-class db.m4.large \
--engine postgres
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--enable-cloudwatch-logs-exports '['"postgresql", "upgrade"]' ^
--db-instance-class db.m4.large ^
--engine postgres
```

RDS API

You can publish PostgreSQL logs with the RDS API. You can call the [ModifyDBInstance](#) action with the following parameters:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

Note

A change to the `CloudwatchLogsExportConfiguration` parameter is always applied to the DB instance immediately. Therefore, the `ApplyImmediately` parameter has no effect.

You can also publish PostgreSQL logs by calling the following RDS API operations:

- [CreateDBInstance](#)
- [RestoreDBInstanceFromDBSnapshot](#)
- [RestoreDBInstanceToPointInTime](#)

Run one of these RDS API operations with the following parameters:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`

- Engine
- DBInstanceClass

Other parameters might be required depending on the operation that you run.

Monitoring Amazon RDS API calls in AWS CloudTrail

AWS CloudTrail is an AWS service that helps you audit your AWS account. AWS CloudTrail is turned on for your AWS account when you create it. For more information about CloudTrail, see the [AWS CloudTrail User Guide](#).

Topics

- [CloudTrail integration with Amazon RDS \(p. 725\)](#)
- [Amazon RDS log file entries \(p. 725\)](#)

CloudTrail integration with Amazon RDS

All Amazon RDS actions are logged by CloudTrail. CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon RDS.

CloudTrail events

CloudTrail captures API calls for Amazon RDS as events. An *event* represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. Events include calls from the Amazon RDS console and from code calls to the Amazon RDS API operations.

Amazon RDS activity is recorded in a CloudTrail event in [Event history](#). You can use the CloudTrail console to view the last 90 days of recorded API activity and events in an AWS Region. For more information, see [Viewing events with CloudTrail event history](#).

CloudTrail trails

For an ongoing record of events in your AWS account, including events for Amazon RDS, create a *trail*. A trail is a configuration that enables delivery of events to a specified Amazon S3 bucket. CloudTrail typically delivers log files within 15 minutes of account activity.

Note

If you don't configure a trail, you can still view the most recent events in the CloudTrail console in [Event history](#).

You can create two types of trails for an AWS account: a trail that applies to all Regions, or a trail that applies to one Region. By default, when you create a trail in the console, the trail applies to all Regions.

Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)
- [Configuring Amazon SNS notifications for CloudTrail](#)
- [Receiving CloudTrail log files from multiple Regions](#) and [Receiving CloudTrail log files from multiple accounts](#)

Amazon RDS log file entries

CloudTrail log files contain one or more log entries. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `CreateDBInstance` action.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
    },
    "eventTime": "2018-07-30T22:14:06Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "CreateDBInstance",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.15.42 Python/3.6.1 Darwin/17.7.0 botocore/1.10.42",
    "requestParameters": {
        "enableCloudwatchLogsExports": [
            "audit",
            "error",
            "general",
            "slowquery"
        ],
        "dBInstanceIdentifier": "test-instance",
        "engine": "mysql",
        "masterUsername": "myawsuser",
        "allocatedStorage": 20,
        "dBInstanceClass": "db.m1.small",
        "masterUserPassword": "*****"
    },
    "responseElements": {
        "dBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance",
        "storageEncrypted": false,
        "preferredBackupWindow": "10:27-10:57",
        "preferredMaintenanceWindow": "sat:05:47-sat:06:17",
        "backupRetentionPeriod": 1,
        "allocatedStorage": 20,
        "storageType": "standard",
        "engineVersion": "8.0.28",
        "dBInstancePort": 0,
        "optionGroupMemberships": [
            {
                "status": "in-sync",
                "optionGroupName": "default:mysql-8-0"
            }
        ],
        "dBParameterGroups": [
            {
                "dBParameterGroupName": "default.mysql8.0",
                "parameterApplyStatus": "in-sync"
            }
        ],
        "monitoringInterval": 0,
        "dBInstanceClass": "db.m1.small",
        "readReplicaDBInstanceIdentifiers": [],
        "dBS subnetGroup": {
            "dBSubnetGroupName": "default",
            "dBSubnetGroupDescription": "default",
            "subnets": [
                {
                    "subnetAvailabilityZone": {"name": "us-east-1b"},
                    "subnetIdentifier": "subnet-cbfff283",
                    "subnetStatus": "available"
                }
            ]
        }
    }
}
```

```

        "subnetStatus": "Active"
    },
    {
        "subnetAvailabilityZone": {"name": "us-east-1e"},
        "subnetIdentifier": "subnet-d7c825e8",
        "subnetStatus": "Active"
    },
    {
        "subnetAvailabilityZone": {"name": "us-east-1f"},
        "subnetIdentifier": "subnet-6746046b",
        "subnetStatus": "Active"
    },
    {
        "subnetAvailabilityZone": {"name": "us-east-1c"},
        "subnetIdentifier": "subnet-bac383e0",
        "subnetStatus": "Active"
    },
    {
        "subnetAvailabilityZone": {"name": "us-east-1d"},
        "subnetIdentifier": "subnet-42599426",
        "subnetStatus": "Active"
    },
    {
        "subnetAvailabilityZone": {"name": "us-east-1a"},
        "subnetIdentifier": "subnet-da327bf6",
        "subnetStatus": "Active"
    }
],
"vpcId": "vpc-136a4c6a",
"subnetGroupStatus": "Complete"
},
"masterUsername": "myawsuser",
"multiAZ": false,
"autoMinorVersionUpgrade": true,
"engine": "mysql",
"caCertificateIdentifier": "rds-ca-2015",
"dbiResourceId": "db-ETDZIIXHEWY5N7GXVC4SH7H5IA",
"dBSecurityGroups": [],
"pendingModifiedValues": [
    "masterUserPassword": "*****",
    "pendingCloudwatchLogsExports": {
        "logTypesToEnable": [
            "audit",
            "error",
            "general",
            "slowquery"
        ]
    }
],
"dBInstanceStatus": "creating",
"publiclyAccessible": true,
"domainMemberships": [],
"copyTagsToSnapshot": false,
"dBInstanceIdentifier": "test-instance",
"licenseModel": "general-public-license",
"iAMDatabaseAuthenticationEnabled": false,
"performanceInsightsEnabled": false,
"vpcSecurityGroups": [
    {
        "status": "active",
        "vpcSecurityGroupId": "sg-f839b688"
    }
],
"requestID": "daf2e3f5-96a3-4df7-a026-863f96db793e",
"eventID": "797163d3-5726-441d-80a7-6eeb7464acd4",

```

```
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

As shown in the `userIdentity` element in the preceding example, every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information about the `userIdentity`, see the [CloudTrail userIdentity element](#). For more information about `CreateDBInstance` and other Amazon RDS actions, see the [Amazon RDS API Reference](#).

Monitoring Amazon RDS for Oracle with Database Activity Streams

By using Database Activity Streams, you can monitor near-real-time streams of database activity.

Topics

- [Overview of Database Activity Streams \(p. 729\)](#)
- [Configuring unified auditing for Oracle Database \(p. 732\)](#)
- [Starting a database activity stream \(p. 732\)](#)
- [Modifying a database activity stream \(p. 734\)](#)
- [Getting the status of a database activity stream \(p. 736\)](#)
- [Stopping a database activity stream \(p. 737\)](#)
- [Monitoring database activity streams \(p. 738\)](#)
- [Managing access to database activity streams \(p. 752\)](#)

Overview of Database Activity Streams

As an RDS for Oracle database administrator, you need to safeguard your database and meet compliance and regulatory requirements. One strategy is to integrate database activity streams with your monitoring tools. In this way, you monitor and set alarms for auditing activity in your Oracle database.

Security threats are both external and internal. To protect against internal threats, you can control administrator access to data streams by configuring the Database Activity Streams feature. RDS for Oracle DBAs don't have access to the collection, transmission, storage, and processing of the streams.

Topics

- [How database activity streams work \(p. 729\)](#)
- [Unified auditing in Oracle Database \(p. 730\)](#)
- [Asynchronous mode for database activity streams \(p. 731\)](#)
- [Requirements for database activity streams \(p. 731\)](#)
- [Region and version availability \(p. 731\)](#)
- [Supported DB instance classes for database activity streams \(p. 731\)](#)

How database activity streams work

Amazon RDS for Oracle pushes activities to an Amazon Kinesis data stream in near real time. The Kinesis stream is created automatically. From Kinesis, you can configure AWS services such as Amazon Kinesis Data Firehose and AWS Lambda to consume the stream and store the data.

Important

Use of the Database Activity Streams feature in Amazon RDS for Oracle is free, but Amazon Kinesis charges for a data stream. For more information, see [Amazon Kinesis Data Streams pricing](#).

You can configure applications for compliance management to consume database activity streams. These applications can use the stream to generate alerts and audit activity on your Oracle database.
[Database Activity Streams](#)

RDS for Oracle supports database activity streams in Multi-AZ deployments. In this case, database activity streams audit both the primary and standby instances.

Unified auditing in Oracle Database

RDS for Oracle doesn't capture database activity by default. You create and manage audit policies in Oracle Database yourself.

Auditing is the monitoring and recording of configured database actions. In an Oracle database, a *unified audit policy* is a named group of audit settings that you can use to audit an aspect of user behavior. A policy can be as simple as auditing the activities of a single user. You can also create complex audit policies that use conditions.

An Oracle database writes audit records, including SYS audit records, to the *unified audit trail*. For example, if an error occurs during an INSERT statement, standard auditing indicates the error number and the SQL that was executed. The audit trail resides in a read-only table in the AUDSYS schema. To access these records, query the UNIFIED_AUDIT_TRAIL data dictionary view.

Typically, you configure database activity streams as follows:

1. Create an Oracle Database audit policy by using the CREATE AUDIT POLICY command.

The Oracle Database generates audit records.

2. Enable the audit policy by using the AUDIT POLICY command.

3. Configure database activity streams.

Only activities that match the Oracle Database audit policies are captured and sent to the Amazon Kinesis data stream. When database activity streams are enabled, an Oracle database administrator can't alter the audit policy or remove audit logs.

To learn more about unified audit policies, see [About Auditing Activities with Unified Audit Policies and AUDIT](#) in the *Oracle Database Security Guide*.

Topics

- [Non-native audit fields \(p. 730\)](#)
- [DB parameter group override \(p. 730\)](#)

Non-native audit fields

When you start a database activity stream, every database event generates a corresponding activity stream event. For example, a database user might run SELECT and INSERT statements. The database audits these events and sends them to an Amazon Kinesis data stream.

The events are represented in the stream as JSON objects. A JSON object contains a DatabaseActivityMonitoringRecord, which contains a databaseActivityEventList array. Predefined fields in the array include class, clientApplication, and command.

Most events in the unified audit trail for Oracle Database map to fields in the RDS data activity stream. For example, the UNIFIED_AUDIT_TRAIL.SQL_TEXT field in unified auditing maps to the commandText field in a database activity stream. However, Oracle Database audit fields such as OS_USERNAME don't map to predefined fields in a database activity stream.

By default, an activity stream doesn't include engine-native audit fields. You can configure RDS for Oracle so that it includes these extra fields in the engineNativeAuditFields JSON object.

DB parameter group override

Typically, you turn on unified auditing in RDS for Oracle by attaching a parameter group. However, Database Activity Streams would require additional configuration. To improve your customer experience, Amazon RDS does the following:

- If you enable an activity stream, RDS for Oracle ignores the auditing parameters in the parameter group.
- If you disable an activity stream, RDS for Oracle stops ignoring the auditing parameters.

Asynchronous mode for database activity streams

Activity streams in RDS for Oracle are always asynchronous. When a database session generates an activity stream event, the session returns to normal activities immediately. In the background, RDS for Oracle makes the activity stream event into a durable record.

If an error occurs in the background task, Amazon RDS generates an event. This event indicates the beginning and end of any time windows where activity stream event records might have been lost. Asynchronous mode favors database performance over the accuracy of the activity stream.

Requirements for database activity streams

In RDS for Oracle, database activity streams have the following requirements and limitations:

- Amazon Kinesis is required for database activity streams.
- AWS Key Management Service (AWS KMS) is required for database activity streams because they are always encrypted.
- Applying additional encryption to your Amazon Kinesis data stream is incompatible with database activity streams, which are already encrypted with your AWS KMS key.
- You create and manage audit policies yourself. Unlike Amazon Aurora, RDS for Oracle doesn't capture database activities by default.
- In a Multi-AZ deployment, start the database activity stream on only the primary DB instance. The activity stream audits both the primary and standby DB instances automatically. No additional steps are required during a failover.
- CDBs aren't supported.
- Oracle read replicas aren't supported.

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability with database activity streams, see [Database activity streams \(p. 85\)](#).

Supported DB instance classes for database activity streams

You can use database activity streams with the following DB instance classes:

- db.m4
- db.m5.*
- db.r4
- db.r5.*
- db.z1d

Note

The memory optimized db.r5 classes, which use the naming pattern db.r5.*instance_size*.tpcthreads_per_core.memratio, aren't supported.

For more information about instance class types, see [DB instance classes \(p. 10\)](#).

Configuring unified auditing for Oracle Database

When you configure unified auditing for use with database activity streams, the following situations are possible:

- Unified auditing isn't configured for your Oracle database.

In this case, create new policies with the CREATE AUDIT POLICY command, and then enable them with the AUDIT POLICY command. The following example creates and enables a policy to monitor users with specific privileges and roles.

```
CREATE AUDIT POLICY table_pol
PRIVILEGES CREATE ANY TABLE, DROP ANY TABLE
ROLES emp_admin, sales_admin;

AUDIT POLICY table_pol;
```

For complete instructions, see [Configuring Audit Policies](#) in the Oracle Database documentation.

- Unified auditing is configured for your Oracle database.

When you enable a database activity stream, RDS for Oracle automatically clears existing audit data. It also revokes audit trail privileges. RDS for Oracle can no longer do the following:

- Purge unified audit trail records.
- Add, delete, or modify the unified audit policy.
- Update the last archived time stamp.

Important

We strongly recommend that you back up your audit data before enabling a database activity stream.

For a description of the UNIFIED_AUDIT_TRAIL view, see [UNIFIED_AUDIT_TRAIL](#). If you have an account with Oracle Support, see [How To Purge The UNIFIED AUDIT TRAIL](#).

Starting a database activity stream

When you start an activity stream for an Oracle DB instance, each database activity event, such as a change or access, generates an activity stream event. SQL commands such as CONNECT and SELECT generate access events. SQL commands such as CREATE and INSERT generate change events.

Important

Turning on an activity stream for an Oracle DB instance clears existing audit data. It also revokes audit trail privileges. When the stream is enabled, RDS for Oracle can no longer do the following:

- Purge unified audit trail records.
- Add, delete, or modify the unified audit policy.
- Update the last archived time stamp.

Console

To start a database activity stream

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

3. Choose the RDS for Oracle instance on which you want to start an activity stream. In a Multi-AZ deployment, start the stream on only the primary instance. The activity stream audits both the primary and the standby instances.
4. For **Actions**, choose **Start activity stream**.

The **Start database activity stream: *name*** window appears, where *name* is your RDS instance.

5. Enter the following settings:

- For **AWS KMS key**, choose a key from the list of AWS KMS keys.

RDS for Oracle uses the KMS key to encrypt the key that in turn encrypts database activity. Choose a KMS key other than the default key. For more information about encryption keys and AWS KMS, see [What is AWS Key Management Service?](#) in the *AWS Key Management Service Developer Guide*.

- For **Database activity events**, choose **Include Oracle native audit fields** to include Oracle-specific audit fields in the stream.
- Choose **Immediately**.

When you choose **Immediately**, the RDS instance restarts right away. If you choose **During the next maintenance window**, the RDS instance doesn't restart right away. In this case, the database activity stream doesn't start until the next maintenance window.

6. Choose **Start database activity stream**.

The status for the Oracle database shows that the activity stream is starting.

Note

If you get the error You can't start a database activity stream in this configuration, check [Supported DB instance classes for database activity streams \(p. 731\)](#) to see whether your RDS instance is using a supported instance class.

AWS CLI

To start database activity streams for an Oracle DB instance, configure the database using the [start-activity-stream](#) AWS CLI command.

- **--resource-arn *arn*** – Specifies the Amazon Resource Name (ARN) of the DB instance.
- **--kms-key-id *key*** – Specifies the KMS key identifier for encrypting messages in the database activity stream. The AWS KMS key identifier is the key ARN, key ID, alias ARN, or alias name for the AWS KMS key.
- **--engine-native-audit-fields-included** – Includes engine-specific unified auditing fields in the data stream. To exclude these fields, specify **--no-engine-native-audit-fields-included** (default).

The following example starts a database activity stream for an Oracle DB instance in asynchronous mode.

For Linux, macOS, or Unix:

```
aws rds start-activity-stream \
--mode async \
--kms-key-id my-kms-key-arn \
--resource-arn my-instance-arn \
--engine-native-audit-fields-included \
--apply-immediately
```

For Windows:

```
aws rds start-activity-stream ^
--mode async ^
--kms-key-id my-kms-key-arn ^
--resource-arn my-instance-arn ^
--engine-native-audit-fields-included ^
--apply-immediately
```

RDS API

To start database activity streams for an Oracle DB instance, configure the instance using the [StartActivityStream](#) operation.

Call the action with the parameters below:

- Region
- KmsKeyId
- ResourceArn
- Mode
- EngineNativeAuditFieldsIncluded

Modifying a database activity stream

You might want to customize your RDS for Oracle audit policy when your activity stream is started. If you don't want to lose time and data by stopping your activity stream, you can change the *audit policy state* to either of the following settings:

Locked (default)

The audit policies in your database are read-only.

Unlocked

The audit policies in your database are read/write.

The basic steps are as follows:

1. Modify the audit policy state to unlocked.
2. Customize your audit policy.
3. Modify the audit policy state to locked.

Console

To modify the audit policy state of your activity stream

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. For **Actions**, choose **Modify database activity stream**.

The **Modify database activity stream: name** window appears, where *name* is your RDS instance.

4. Choose either of the following options:

Locked

When you lock your audit policy, it becomes read-only. You can't edit your audit policy unless you unlock the policy or stop the activity stream.

Unlocked

When you unlock your audit policy, it becomes read/write. You can edit your audit policy while the activity stream is started.

5. Choose **Modify DB activity stream**.

The status for the Oracle database shows **Configuring activity stream**.

6. (Optional) Choose the DB instance link. Then choose the **Configuration** tab.

The **Audit policy status** field shows one of the following values:

- **Locked**
- **Unlocked**
- **Locking policy**
- **Unlocking policy**

AWS CLI

To modify the activity stream state for an Oracle DB instance, use the [modify-activity-stream](#) AWS CLI command.

Option	Required?	Description
--resource-arn <i>my-instance-ARN</i>	Yes	The Amazon Resource Name (ARN) of your RDS for Oracle DB instance.
--audit-policy-state	No	The new state of the audit policy for the database activity stream on your instance: locked or unlocked.

The following example unlocks the audit policy for the activity stream started on *my-instance-ARN*.

For Linux, macOS, or Unix:

```
aws rds modify-activity-stream \
--resource-arn my-instance-ARN \
--audit-policy-state unlocked
```

For Windows:

```
aws rds modify-activity-stream ^
--resource-arn my-instance-ARN ^
--audit-policy-state unlocked
```

The following example describes the instance *my-instance*. The partial sample output shows that the audit policy is unlocked.

```
aws rds describe-db-instances --db-instance-identifier my-instance

{
    "DBInstances": [
        {
            ...
            "Engine": "oracle-ee",
            ...
            "ActivityStreamStatus": "started",
```

```
    "ActivityStreamKmsKeyId": "ab12345e-1111-2bc3-12a3-ab1cd12345e",
    "ActivityStreamKinesisStreamName": "aws-rds-das-db-AB1CDEFG23GHIJK4LMNOPQRST",
    "ActivityStreamMode": "async",
    "ActivityStreamEngineNativeAuditFieldsIncluded": true,
    "ActivityStreamPolicyStatus": "unlocked",
    ...
]
}
```

RDS API

To modify the policy state of your database activity stream, use the [ModifyActivityStream](#) operation.

Call the action with the parameters below:

- `AuditPolicyState`
- `ResourceArn`

Getting the status of a database activity stream

You can get the status of an activity stream for your RDS for Oracle DB instance using the console or AWS CLI.

Console

To get the status of a database activity stream

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance link.
3. Choose the **Configuration** tab, and check **Database activity stream** for status.

AWS CLI

You can get the activity stream configuration for a database as the response to a [describe-db-instances](#) CLI request.

The following example describes *my-instance*.

```
aws rds --region my-region describe-db-instances --db-instance-identifier my-db
```

The following example shows a JSON response. The following fields are shown:

- `ActivityStreamKinesisStreamName`
- `ActivityStreamKmsKeyId`
- `ActivityStreamStatus`
- `ActivityStreamMode`
- `ActivityStreamPolicyStatus`

```
{
  "DBInstances": [
    {
      ...
      "Engine": "oracle-ee",
    }
  ]
}
```

```
    ...
    "ActivityStreamStatus": "starting",
    "ActivityStreamKmsKeyId": "ab12345e-1111-2bc3-12a3-ab1cd12345e",
    "ActivityStreamKinesisStreamName": "aws-rds-das-db-AB1CDEFG23GHIJK4LMNOPQRST",
    "ActivityStreamMode": "async",
    "ActivityStreamEngineNativeAuditFieldsIncluded": true,
    "ActivityStreamPolicyStatus": "locked",
    ...
}
]
```

RDS API

You can get the activity stream configuration for a database as the response to a [DescribeDBInstances](#) operation.

Stopping a database activity stream

You can stop an activity stream using the console or AWS CLI.

If you delete your RDS for Oracle DB instance, the activity stream is stopped and the underlying Amazon Kinesis stream is deleted automatically.

Console

To turn off an activity stream

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose a database that you want to stop the database activity stream for.
4. For **Actions**, choose **Stop activity stream**. The **Database Activity Stream** window appears.
 - a. Choose **Immediately**.

When you choose **Immediately**, the RDS instance restarts right away. If you choose **During the next maintenance window**, the RDS instance doesn't restart right away. In this case, the database activity stream doesn't stop until the next maintenance window.

- b. Choose **Continue**.

AWS CLI

To stop database activity streams for your database, configure the DB instance using the AWS CLI command [stop-activity-stream](#). Identify the AWS Region for the DB instance using the `--region` parameter. The `--apply-immediately` parameter is optional.

For Linux, macOS, or Unix:

```
aws rds --region MY_REGION \
  stop-activity-stream \
  --resource-arn MY_DB_ARN \
  --apply-immediately
```

For Windows:

```
aws rds --region MY_REGION ^
  stop-activity-stream ^
  --resource-arn MY_DB_ARN ^
```

--apply-immediately

RDS API

To stop database activity streams for your database, configure the DB instance using the [StopActivityStream](#) operation. Identify the AWS Region for the DB instance using the Region parameter. The ApplyImmediately parameter is optional.

Monitoring database activity streams

Database activity streams monitor and report activities. The stream of activity is collected and transmitted to Amazon Kinesis. From Kinesis, you can monitor the activity stream, or other services and applications can consume the activity stream for further analysis. You can find the underlying Kinesis stream name by using the AWS CLI command `describe-db-instances` or the RDS API `DescribeDBInstances` operation.

Amazon RDS manages the Kinesis stream for you as follows:

- Amazon RDS creates the Kinesis stream automatically with a 24-hour retention period.
- Amazon RDS scales the Kinesis stream if necessary.
- If you stop the database activity stream or delete the DB instance, Amazon RDS deletes the Kinesis stream.

The following categories of activity are monitored and put in the activity stream audit log:

- **SQL commands** – All SQL commands are audited, and also prepared statements, built-in functions, and functions in PL/SQL. Calls to stored procedures are audited. Any SQL statements issued inside stored procedures or functions are also audited.
- **Other database information** – Activity monitored includes the full SQL statement, the row count of affected rows from DML commands, accessed objects, and the unique database name. Database activity streams also monitor the bind variables and stored procedure parameters.

Important

The full SQL text of each statement is visible in the activity stream audit log, including any sensitive data. However, database user passwords are redacted if Oracle can determine them from the context, such as in the following SQL statement.

ALTER ROLE role-name WITH password

- **Connection information** – Activity monitored includes session and network information, the server process ID, and exit codes.

If an activity stream has a failure while monitoring your DB instance, you are notified through RDS events.

Topics

- [Accessing an activity stream from Kinesis \(p. 738\)](#)
- [Audit log contents and examples \(p. 739\)](#)
- [Processing a database activity stream using the AWS SDK \(p. 752\)](#)

Accessing an activity stream from Kinesis

When you enable an activity stream for a database, a Kinesis stream is created for you. From Kinesis, you can monitor your database activity in real time. To further analyze database activity, you can

connect your Kinesis stream to consumer applications. You can also connect the stream to compliance management applications such as IBM's Security Guardium or Imperva's SecureSphere Database Audit and Protection.

You can access your Kinesis stream either from the RDS console or the Kinesis console.

To access an activity stream from Kinesis using the RDS console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the RDS for Oracle instance on which you started an activity stream.
4. Choose **Configuration**.
5. Under **Database activity stream**, choose the link under **Kinesis stream**.
6. In the Kinesis console, choose **Monitoring** to begin observing the database activity.

To access an activity stream from Kinesis using the Kinesis console

1. Open the Kinesis console at <https://console.aws.amazon.com/kinesis>.
2. Choose your activity stream from the list of Kinesis streams.

An activity stream's name includes the prefix aws-rds-das-db- followed by the resource ID of the database. The following is an example.

```
aws-rds-das-db-NHV0V4PCLWHGF52NP
```

To use the Amazon RDS console to find the resource ID for the database, choose your DB instance from the list of databases, and then choose the **Configuration** tab.

To use the AWS CLI to find the full Kinesis stream name for an activity stream, use a [describe-db-instances](#) CLI request and note the value of ActivityStreamKinesisStreamName in the response.

3. Choose **Monitoring** to begin observing the database activity.

For more information about using Amazon Kinesis, see [What Is Amazon Kinesis Data Streams?](#).

Audit log contents and examples

Monitored events are represented in the database activity stream as JSON strings. The structure consists of a JSON object containing a **DatabaseActivityMonitoringRecord**, which in turn contains a **databaseActivityEventList** array of activity events.

Topics

- [Examples of an audit log for an activity stream \(p. 739\)](#)
- [DatabaseActivityMonitoringRecords JSON object \(p. 745\)](#)
- [databaseActivityEvents JSON Object \(p. 745\)](#)
- [databaseActivityEventList JSON array \(p. 747\)](#)

Examples of an audit log for an activity stream

Following are sample decrypted JSON audit logs of activity event records.

Example Activity event record of a CONNECT SQL statement

Following is an activity event record of a login with the use of a CONNECT SQL statement (command) by a JDBC Thin Client (clientApplication).

```
{  
    "class": "Standard",  
    "clientApplication": "JDBC Thin Client",  
    "command": "LOGON",  
    "commandText": null,  
    "dbid": "0123456789",  
    "databaseName": "ORCL",  
    "dbProtocol": "oracle",  
    "dbUserName": "TEST",  
    "endTime": null,  
    "errorMessage": null,  
    "exitCode": 0,  
    "logTime": "2021-01-15 00:15:36.233787",  
    "netProtocol": "tcp",  
    "objectName": null,  
    "objectType": null,  
    "paramList": [],  
    "pid": 17904,  
    "remoteHost": "123.456.789.012",  
    "remotePort": "25440",  
    "rowCount": null,  
    "serverHost": "987.654.321.098",  
    "serverType": "oracle",  
    "serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",  
    "serviceName": "oracle-ee",  
    "sessionId": 987654321,  
    "startTime": null,  
    "statementId": 1,  
    "substatementId": null,  
    "transactionId": "0000000000000000",  
    "engineNativeAuditFields": {  
        "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",  
        "FGA_POLICY_NAME": null,  
        "DV_OBJECT_STATUS": null,  
        "SYSTEM_PRIVILEGE_USED": "CREATE SESSION",  
        "OLS_LABEL_COMPONENT_TYPE": null,  
        "XS_SESSIONID": null,  
        "ADDITIONAL_INFO": null,  
        "INSTANCE_ID": 1,  
        "DBID": 123456789  
        "DV_COMMENT": null,  
        "RMAN_SESSION_STAMP": null,  
        "NEW_NAME": null,  
        "DV_ACTION_NAME": null,  
        "OLS_PROGRAM_UNIT_NAME": null,  
        "OLS_STRING_LABEL": null,  
        "RMAN_SESSION_RECID": null,  
        "OBJECT_PRIVILEGES": null,  
        "OLS_OLD_VALUE": null,  
        "XS_TARGET_PRINCIPAL_NAME": null,  
        "XS_NS_ATTRIBUTE": null,  
        "XS_NS_NAME": null,  
        "DBLINK_INFO": null,  
        "AUTHENTICATION_TYPE": "(TYPE\u003dDATABASE));(CLIENT ADDRESS\u003d((ADDRESS  
\u003dPROTOCOL\u003dtcp)(HOST\u003d205.251.233.183)(PORT\u003d25440)));",  
        "OBJECT_EDITION": null,  
        "OLS_PRIVILEGES_GRANTED": null,  
        "EXCLUDED_USER": null,  
        "DV_ACTION_OBJECT_NAME": null,  
        "OLS_LABEL_COMPONENT_NAME": null,  
    }  
}
```

```
"EXCLUDED_SCHEMA": null,
"DP_TEXT_PARAMETERS1": null,
"XS_USER_NAME": null,
"XS_ENABLED_ROLE": null,
"XS_NS_ATTRIBUTE_NEW_VAL": null,
"DIRECT_PATH_NUM_COLUMNS_LOADED": null,
"AUDIT_OPTION": null,
"DV_EXTENDED_ACTION_CODE": null,
"XS_PACKAGE_NAME": null,
"OLS_NEW_VALUE": null,
"DV_RETURN_CODE": null,
"XS_CALLBACK_EVENT_TYPE": null,
"USERHOST": "a1b2c3d4e5f6.amazon.com",
"GLOBAL_USERID": null,
"CLIENT_IDENTIFIER": null,
"RMAN_OPERATION": null,
"TERMINAL": "unknown",
"OS_USERNAME": "sumepate",
"OLS_MAX_READ_LABEL": null,
"XS_PROXY_USER_NAME": null,
"XS_DATASEC_POLICY_NAME": null,
"DV_FACTOR_CONTEXT": null,
"OLS_MAX_WRITE_LABEL": null,
"OLS_PARENT_GROUP_NAME": null,
"EXCLUDED_OBJECT": null,
"DV_RULE_SET_NAME": null,
"EXTERNAL_USERID": null,
"EXECUTION_ID": null,
"ROLE": null,
"PROXY_SESSIONID": 0,
"DP_BOOLEAN_PARAMETERS1": null,
"OLS_POLICY_NAME": null,
"OLS_GRANTEE": null,
"OLS_MIN_WRITE_LABEL": null,
"APPLICATION_CONTEXTS": null,
"XS_SCHEMA_NAME": null,
"DV_GRANTEE": null,
"XS_COOKIE": null,
"DBPROXY_USERNAME": null,
"DV_ACTION_CODE": null,
"OLS_PRIVILEGES_USED": null,
"RMAN_DEVICE_TYPE": null,
"XS_NS_ATTRIBUTE_OLD_VAL": null,
"TARGET_USER": null,
"XS_ENTITY_TYPE": null,
"ENTRY_ID": 1,
"XS_PROCEDURE_NAME": null,
"XS_INACTIVITY_TIMEOUT": null,
"RMAN_OBJECT_TYPE": null,
"SYSTEM_PRIVILEGE": null,
"NEW_SCHEMA": null,
"SCN": 5124715
}
}
```

Note

If a database activity stream isn't enabled, then the last field in the JSON document is "engineNativeAuditFields": {}.

Example Activity event record of a CREATE TABLE statement

Following is an example of a CREATE TABLE event for your Oracle database.

```
{
```

```

"class": "Standard",
"clientApplication": "sqlplus@ip-12-34-5-678 (TNS V1-V3)",
"command": "CREATE TABLE",
"commandText": "CREATE TABLE persons(\n    person_id NUMBER GENERATED BY DEFAULT AS\n    IDENTITY,\n    first_name VARCHAR2(50) NOT NULL,\n    last_name VARCHAR2(50) NOT NULL,\n    PRIMARY KEY(person_id)\n)",
"dbid": "0123456789",
"databaseName": "ORCL",
"dbProtocol": "oracle",
"dbUserName": "TEST",
"endTime": null,
"errorMessage": null,
"exitCode": 0,
"logTime": "2021-01-15 00:22:49.535239",
"netProtocol": "beq",
"objectName": "PERSONS",
"objectType": "TEST",
"paramList": [],
"pid": 17687,
"remoteHost": "123.456.789.0",
"remotePort": null,
"rowCount": null,
"serverHost": "987.654.321.01",
"serverType": "oracle",
"serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",
"serviceName": "oracle-ee",
"sessionId": 1234567890,
"startTime": null,
"statementId": 43,
"substatementId": null,
"transactionId": "090011007F0D0000",
"engineNativeAuditFields": {
    "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",
    "FGA_POLICY_NAME": null,
    "DV_OBJECT_STATUS": null,
    "SYSTEM_PRIVILEGE_USED": "CREATE SEQUENCE, CREATE TABLE",
    "OLS_LABEL_COMPONENT_TYPE": null,
    "XS_SESSIONID": null,
    "ADDITIONAL_INFO": null,
    "INSTANCE_ID": 1,
    "DV_COMMENT": null,
    "RMAN_SESSION_STAMP": null,
    "NEW_NAME": null,
    "DV_ACTION_NAME": null,
    "OLS_PROGRAM_UNIT_NAME": null,
    "OLS_STRING_LABEL": null,
    "RMAN_SESSION_RECID": null,
    "OBJECT_PRIVILEGES": null,
    "OLS_OLD_VALUE": null,
    "XS_TARGET_PRINCIPAL_NAME": null,
    "XS_NS_ATTRIBUTE": null,
    "XS_NS_NAME": null,
    "DBLINK_INFO": null,
    "AUTHENTICATION_TYPE": "(TYPE\u003d(DATABASE));(CLIENT ADDRESS\u003d((PROTOCOL
\u003dbeq)(HOST\u003d123.456.789.0)));",
    "OBJECT_EDITION": null,
    "OLS_PRIVILEGES_GRANTED": null,
    "EXCLUDED_USER": null,
    "DV_ACTION_OBJECT_NAME": null,
    "OLS_LABEL_COMPONENT_NAME": null,
    "EXCLUDED_SCHEMA": null,
    "DP_TEXT_PARAMETERS1": null,
    "XS_USER_NAME": null,
    "XS_ENABLED_ROLE": null,
    "XS_NS_ATTRIBUTE_NEW_VAL": null,
    "DIRECT_PATH_NUM_COLUMNS_LOADED": null,
}

```

```

    "AUDIT_OPTION": null,
    "DV_EXTENDED_ACTION_CODE": null,
    "XS_PACKAGE_NAME": null,
    "OLS_NEW_VALUE": null,
    "DV_RETURN_CODE": null,
    "XS_CALLBACK_EVENT_TYPE": null,
    "USERHOST": "ip-10-13-0-122",
    "GLOBAL_USERID": null,
    "CLIENT_IDENTIFIER": null,
    "RMAN_OPERATION": null,
    "TERMINAL": "pts/1",
    "OS_USERNAME": "rdsdb",
    "OLS_MAX_READ_LABEL": null,
    "XS_PROXY_USER_NAME": null,
    "XS_DATASEC_POLICY_NAME": null,
    "DV_FACTOR_CONTEXT": null,
    "OLS_MAX_WRITE_LABEL": null,
    "OLS_PARENT_GROUP_NAME": null,
    "EXCLUDED_OBJECT": null,
    "DV_RULE_SET_NAME": null,
    "EXTERNAL_USERID": null,
    "EXECUTION_ID": null,
    "ROLE": null,
    "PROXY_SESSIONID": 0,
    "DP_BOOLEAN_PARAMETERS1": null,
    "OLS_POLICY_NAME": null,
    "OLS_GRANTEE": null,
    "OLS_MIN_WRITE_LABEL": null,
    "APPLICATION_CONTEXTS": null,
    "XS_SCHEMA_NAME": null,
    "DV_GRANTEE": null,
    "XS_COOKIE": null,
    "DBPROXY_USERNAME": null,
    "DV_ACTION_CODE": null,
    "OLS_PRIVILEGES_USED": null,
    "RMAN_DEVICE_TYPE": null,
    "XS_NS_ATTRIBUTE_OLD_VAL": null,
    "TARGET_USER": null,
    "XS_ENTITY_TYPE": null,
    "ENTRY_ID": 12,
    "XS_PROCEDURE_NAME": null,
    "XS_INACTIVITY_TIMEOUT": null,
    "RMAN_OBJECT_TYPE": null,
    "SYSTEM_PRIVILEGE": null,
    "NEW_SCHEMA": null,
    "SCN": 5133083
}
}

```

Example Activity event record of a SELECT statement

Following is an example of a SELECT event.

```
{
  "class": "Standard",
  "clientApplication": "sqlplus@ip-12-34-5-678 (TNS V1-V3)",
  "command": "SELECT",
  "commandText": "select count(*) from persons",
  "databaseName": "1234567890",
  "dbProtocol": "oracle",
  "dbUserName": "TEST",
  "endTime": null,
  "errorMessage": null,
  "exitCode": 0,
}
```

```
"logTime": "2021-01-15 00:25:18.850375",
"netProtocol": "beq",
"objectName": "PERSONS",
"objectType": "TEST",
"paramList": [],
"pid": 17687,
"remoteHost": "123.456.789.0",
"remotePort": null,
"rowCount": null,
"serverHost": "987.654.321.09",
"serverType": "oracle",
"serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",
"serviceName": "oracle-ee",
"sessionId": 1080639707,
"startTime": null,
"statementId": 44,
"substatementId": null,
"transactionId": null,
"engineNativeAuditFields": {
    "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",
    "FGA_POLICY_NAME": null,
    "DV_OBJECT_STATUS": null,
    "SYSTEM_PRIVILEGE_USED": null,
    "OLS_LABEL_COMPONENT_TYPE": null,
    "XS_SESSIONID": null,
    "ADDITIONAL_INFO": null,
    "INSTANCE_ID": 1,
    "DV_COMMENT": null,
    "RMAN_SESSION_STAMP": null,
    "NEW_NAME": null,
    "DV_ACTION_NAME": null,
    "OLS_PROGRAM_UNIT_NAME": null,
    "OLS_STRING_LABEL": null,
    "RMAN_SESSION_RECID": null,
    "OBJECT_PRIVILEGES": null,
    "OLS_OLD_VALUE": null,
    "XS_TARGET_PRINCIPAL_NAME": null,
    "XS_NS_ATTRIBUTE": null,
    "XS_NS_NAME": null,
    "DBLINK_INFO": null,
    "AUTHENTICATION_TYPE": "(TYPE\u003d(DATABASE));(CLIENT ADDRESS\u003d((PROTOCOL
\u003dbeq)(HOST\u003d123.456.789.0)));",
    "OBJECT_EDITION": null,
    "OLS_PRIVILEGES_GRANTED": null,
    "EXCLUDED_USER": null,
    "DV_ACTION_OBJECT_NAME": null,
    "OLS_LABEL_COMPONENT_NAME": null,
    "EXCLUDED_SCHEMA": null,
    "DP_TEXT_PARAMETERS1": null,
    "XS_USER_NAME": null,
    "XS_ENABLED_ROLE": null,
    "XS_NS_ATTRIBUTE_NEW_VAL": null,
    "DIRECT_PATH_NUM_COLUMNS_LOADED": null,
    "AUDIT_OPTION": null,
    "DV_EXTENDED_ACTION_CODE": null,
    "XS_PACKAGE_NAME": null,
    "OLS_NEW_VALUE": null,
    "DV_RETURN_CODE": null,
    "XS_CALLBACK_EVENT_TYPE": null,
    "USERHOST": "ip-12-34-5-678",
    "GLOBAL_USERID": null,
    "CLIENT_IDENTIFIER": null,
    "RMAN_OPERATION": null,
    "TERMINAL": "pts/1",
    "OS_USERNAME": "rdsdb",
    "OLS_MAX_READ_LABEL": null,
```

```

    "XS_PROXY_USER_NAME": null,
    "XS_DATASEC_POLICY_NAME": null,
    "DV_FACTOR_CONTEXT": null,
    "OLS_MAX_WRITE_LABEL": null,
    "OLS_PARENT_GROUP_NAME": null,
    "EXCLUDED_OBJECT": null,
    "DV_RULE_SET_NAME": null,
    "EXTERNAL_USERID": null,
    "EXECUTION_ID": null,
    "ROLE": null,
    "PROXY_SESSIONID": 0,
    "DP_BOOLEAN_PARAMETERS1": null,
    "OLS_POLICY_NAME": null,
    "OLS_GRANTEE": null,
    "OLS_MIN_WRITE_LABEL": null,
    "APPLICATION_CONTEXTS": null,
    "XS_SCHEMA_NAME": null,
    "DV_GRANTEE": null,
    "XS_COOKIE": null,
    "DBPROXY_USERNAME": null,
    "DV_ACTION_CODE": null,
    "OLS_PRIVILEGES_USED": null,
    "RMAN_DEVICE_TYPE": null,
    "XS_NS_ATTRIBUTE_OLD_VAL": null,
    "TARGET_USER": null,
    "XS_ENTITY_TYPE": null,
    "ENTRY_ID": 13,
    "XS_PROCEDURE_NAME": null,
    "XS_INACTIVITY_TIMEOUT": null,
    "RMAN_OBJECT_TYPE": null,
    "SYSTEM_PRIVILEGE": null,
    "NEW_SCHEMA": null,
    "SCN": 5136972
}
}

```

DatabaseActivityMonitoringRecords JSON object

The database activity event records are in a JSON object that contains the following information.

JSON Field	Data Type	Description
type	string	The type of JSON record. The value is DatabaseActivityMonitoringRecords.
version	string	The version of the database activity monitoring records. Oracle DB uses version 1.3. This version introduces the engineNativeAuditFields JSON object.
databaseActivityEvents <small>(String)</small>	string	A JSON object containing the activity events.
key	string	An encryption key you use to decrypt the databaseActivityEventList (p. 747) databaseActivityEventList JSON array.

databaseActivityEvents JSON Object

The databaseActivityEvents JSON object contains the following information.

Top-level fields in JSON record

Each event in the audit log is wrapped inside a record in JSON format. This record contains the following fields.

type

This field always has the value `DatabaseActivityMonitoringRecords`.

version

This field represents the version of the database activity stream data protocol or contract. It defines which fields are available.

databaseActivityEvents

An encrypted string representing one or more activity events. It's represented as a base64 byte array. When you decrypt the string, the result is a record in JSON format with fields as shown in the examples in this section.

key

The encrypted data key used to encrypt the `databaseActivityEvents` string. This is the same AWS KMS key that you provided when you started the database activity stream.

The following example shows the format of this record.

```
{
  "type": "DatabaseActivityMonitoringRecords",
  "version": "1.3",
  "databaseActivityEvents": "encrypted audit records",
  "key": "encrypted key"
}
```

Take the following steps to decrypt the contents of the `databaseActivityEvents` field:

1. Decrypt the value in the `key` JSON field using the KMS key you provided when starting database activity stream. Doing so returns the data encryption key in clear text.
2. Base64-decode the value in the `databaseActivityEvents` JSON field to obtain the ciphertext, in binary format, of the audit payload.
3. Decrypt the binary ciphertext with the data encryption key that you decoded in the first step.
4. Decompress the decrypted payload.
 - The encrypted payload is in the `databaseActivityEvents` field.
 - The `databaseActivityEventList` field contains an array of audit records. The `type` fields in the array can be `record` or `heartbeat`.

The audit log activity event record is a JSON object that contains the following information.

JSON Field	Data Type	Description
<code>type</code>	string	The type of JSON record. The value is <code>DatabaseActivityMonitoringRecord</code> .
<code>instanceId</code>	string	The DB instance resource identifier. It corresponds to the DB instance attribute <code>DbiResourceId</code> .
<code>databaseActivityEventList</code> (Page 747)		An array of activity audit records or heartbeat messages.

databaseActivityEventList JSON array

The audit log payload is an encrypted databaseActivityEventList JSON array. The following table lists alphabetically the fields for each activity event in the decrypted DatabaseActivityEventList array of an audit log.

When unified auditing is enabled in Oracle Database, the audit records are populated in this new audit trail. The UNIFIED_AUDIT_TRAIL view displays audit records in tabular form by retrieving the audit records from the audit trail. When you start a database activity stream, a column in UNIFIED_AUDIT_TRAIL maps to a field in the databaseActivityEventList array.

Important

The event structure is subject to change. Amazon RDS might add new fields to activity events in the future. In applications that parse the JSON data, make sure that your code can ignore or take appropriate actions for unknown field names.

databaseActivityEventList fields for Amazon RDS for Oracle

Field	Data Type	Source	Description
class	string	AUDIT_TYPE column in UNIFIED_AUDIT_TRAIL	<p>The class of activity event. This corresponds to the AUDIT_TYPE column in the UNIFIED_AUDIT_TRAIL view. Valid values for Amazon RDS for Oracle are the following:</p> <ul style="list-style-type: none"> • Standard • FineGrainedAudit • XS • Database Vault • Label Security • RMAN_AUDIT • Datapump • Direct path API <p>For more information, see UNIFIED_AUDIT_TRAIL in the Oracle documentation.</p>
clientApplication	string	CLIENT_PROGRAM_NAME in UNIFIED_AUDIT_TRAIL	The application the client used to connect as reported by the client. The client doesn't have to provide this information, so the value can be null. A sample value is JDBC Thin Client.
command	string	ACTION_NAME column in UNIFIED_AUDIT_TRAIL	Name of the action executed by the user. To understand the complete action, read both the command name and the AUDIT_TYPE value. A sample value is ALTER DATABASE.

Field	Data Type	Source	Description
commandText	string	SQL_TEXT column in UNIFIED_AUDIT_TRAIL	The SQL statement associated with the event. A sample value is ALTER DATABASE BEGIN BACKUP.
databaseName	string	NAME column in V\$DATABASE	The name of the database.
dbid	number	DBID column in UNIFIED_AUDIT_TRAIL	Numerical identifier for the database. A sample value is 1559204751.
dbProtocol	string	N/A	The database protocol. In this beta, the value is oracle.
dbUserName	string	DBUSERNAME column in UNIFIED_AUDIT_TRAIL	Name of the database user whose actions were audited. A sample value is RDSADMIN.
endTime	string	N/A	This field isn't used for RDS for Oracle and is always null.

Field	Data Type	Source	Description
engineNativeAuditFields	object	UNIFIED_AUDIT_TRAIL	<p>By default, this object is empty. When you start the activity stream with the --engine-native-audit-fields-included option, this object includes the following columns and their values:</p> <pre> ADDITIONAL_INFO APPLICATION_CONTEXTS AUDIT_OPTION AUTHENTICATION_TYPE CLIENT_IDENTIFIER CURRENT_USER DBLINK_INFO DBPROXY_USERNAME DIRECT_PATH_NUM_COLUMNS_LOADED DP_BOOLEAN_PARAMETERS1 DP_TEXT_PARAMETERS1 DV_ACTION_CODE DV_ACTION_NAME DV_ACTION_OBJECT_NAME DV_COMMENT DV_EXTENDED_ACTION_CODE DV_FACTOR_CONTEXT DV_GRANTEE DV_OBJECT_STATUS DV_RETURN_CODE DV_RULE_SET_NAME ENTRY_ID EXCLUDED_OBJECT EXCLUDED_SCHEMA EXCLUDED_USER EXECUTION_ID EXTERNAL_USERID FGA_POLICY_NAME GLOBAL_USERID INSTANCE_ID KSACL_SERVICE_NAME KSACL_SOURCE_LOCATION KSACL_USER_NAME NEW_NAME NEW_SCHEMA OBJECT_EDITION OBJECT_PRIVILEGES OLS_GRANTEE OLS_LABEL_COMPONENT_NAME OLS_LABEL_COMPONENT_TYPE OLS_MAX_READ_LABEL OLS_MAX_WRITE_LABEL OLS_MIN_WRITE_LABEL OLS_NEW_VALUE OLS_OLD_VALUE OLS_PARENT_GROUP_NAME OLS_POLICY_NAME OLS_PRIVILEGES_GRANTED OLS_PRIVILEGES_USED OLS_PROGRAM_UNIT_NAME OLS_STRING_LABEL </pre>

Field	Data Type	Source	Description
			OS_USERNAME PROTOCOL_ACTION_NAME PROTOCOL_MESSAGE PROTOCOL_RETURN_CODE PROTOCOL_SESSION_ID PROTOCOL_USERHOST PROXY_SESSIONID RLS_INFO RMAN_DEVICE_TYPE RMAN_OBJECT_TYPE RMAN_OPERATION RMAN_SESSION_RECID RMAN_SESSION_STAMP ROLE SCN SYSTEM_PRIVILEGE SYSTEM_PRIVILEGE_USED TARGET_USER TERMINAL UNIFIED_AUDIT_POLICIES USERHOST XS_CALLBACK_EVENT_TYPE XS_COOKIE XS_DATASEC_POLICY_NAME XS_ENABLED_ROLE XS_ENTITY_TYPE XS_INACTIVITY_TIMEOUT XS_NS_ATTRIBUTE XS_NS_ATTRIBUTE_NEW_VAL XS_NS_ATTRIBUTE_OLD_VAL XS_NS_NAME XS_PACKAGE_NAME XS_PROCEDURE_NAME XS_PROXY_USER_NAME XS_SCHEMA_NAME XS_SESSIONID XS_TARGET_PRINCIPAL_NAME XS_USER_NAME
			For more information, see UNIFIED_AUDIT_TRAIL in the Oracle Database documentation.
errorMessage	string	N/A	This field isn't used for RDS for Oracle and is always null.
exitCode	number	RETURN_CODE column in UNIFIED_AUDIT_TRAIL	Oracle Database error code generated by the action. If the action succeeded, the value is 0.
logTime	string	EVENT_TIMESTAMP_UTC column in UNIFIED_AUDIT_TRAIL	Timestamp of the creation of the audit trail entry. A sample value is 2020-11-27 06:56:14.981404.

Field	Data Type	Source	Description
netProtocol	string	AUTHENTICATION_TYPE column in UNIFIED_AUDIT_TRAIL	The network communication protocol. A sample value is TCP.
objectName	string	OBJECT_NAME column in UNIFIED_AUDIT_TRAIL	The name of the object affected by the action. A sample value is employees.
objectType	string	OBJECT_SCHEMA column in UNIFIED_AUDIT_TRAIL	The schema name of object affected by the action. A sample value is hr.
paramList	list	SQL_BINDS column in UNIFIED_AUDIT_TRAIL	The list of bind variables, if any, associated with SQL_TEXT. A sample value is parameter_1,parameter_2.
pid	number	OS_PROCESS column in UNIFIED_AUDIT_TRAIL	Operating system process identifier of the Oracle database process. A sample value is 22396.
remoteHost	string	AUTHENTICATION_TYPE column in UNIFIED_AUDIT_TRAIL	Either the client IP address or name of the host from which the session was spawned. A sample value is 123.456.789.123.
remotePort	string	AUTHENTICATION_TYPE column in UNIFIED_AUDIT_TRAIL	The client port number. A typical value in Oracle Database environments is 1521.
rowCount	number	N/A	This field isn't used for RDS for Oracle and is always null.
serverHost	string	Database host	The IP address of the database server host. A sample value is 123.456.789.123.
serverType	string	N/A	The database server type. The value is always ORACLE.
serverVersion	string	Database host	The Amazon RDS for Oracle version, Release Update (RU), and Release Update Revision (RUR). A sample value is 19.0.0.0.ru-2020-01.rur-2020-01.r1
serviceName	string	Database host	The name of the service. A sample value is oracle-ee.
sessionId	number	SESSIONID column in UNIFIED_AUDIT_TRAIL	The session identifier of the audit. An example is 1894327130.

Field	Data Type	Source	Description
startTime	string	N/A	This field isn't used for RDS for Oracle and is always null.
statementId	number	STATEMENT_ID column in UNIFIED_AUDIT_TRAIL	Numeric ID for each statement run. A statement can cause many actions. A sample value is 142197.
substatementId	N/A	N/A	This field isn't used for RDS for Oracle and is always null.
transactionId	string	TRANSACTION_ID column in UNIFIED_AUDIT_TRAIL	The identifier of the transaction in which the object is modified. A sample value is 02000800D5030000.

Processing a database activity stream using the AWS SDK

You can programmatically process an activity stream by using the AWS SDK.

Managing access to database activity streams

Any user with appropriate AWS Identity and Access Management (IAM) role privileges for database activity streams can create, start, stop, and modify the activity stream settings for a DB instance. These actions are included in the audit log of the stream. For best compliance practices, we recommend that you don't provide these privileges to DBAs.

You set access to database activity streams using IAM policies. For more information about RDS for Oracle authentication, see [Identity and access management for Amazon RDS \(p. 2016\)](#). For more information about creating IAM policies, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#).

Example Policy to allow configuring database activity streams

To give users fine-grained access to modify activity streams, use the service-specific operation context keys `rds:StartActivityStream` and `rds:StopActivityStream` in an IAM policy. The following IAM policy example allows a user or role to configure activity streams.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigureActivityStreams",
            "Effect": "Allow",
            "Action": [
                "rds:StartActivityStream",
                "rds:StopActivityStream"
            ],
            "Resource": "*",
        }
    ]
}
```

Example Policy to allow starting database activity streams

The following IAM policy example allows a user or role to start activity streams.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowStartActivityStreams",  
            "Effect": "Allow",  
            "Action": "rds:StartActivityStream",  
            "Resource": "*"  
        }  
    ]  
}
```

Example Policy to allow stopping database activity streams

The following IAM policy example allows a user or role to stop activity streams.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowStopActivityStreams",  
            "Effect": "Allow",  
            "Action": "rds:StopActivityStream",  
            "Resource": "*"  
        }  
    ]  
}
```

Example Policy to deny starting database activity streams

The following IAM policy example prevents a user or role from starting activity streams.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DenyStartActivityStreams",  
            "Effect": "Deny",  
            "Action": "rds:StartActivityStream",  
            "Resource": "*"  
        }  
    ]  
}
```

Example Policy to deny stopping database activity streams

The following IAM policy example prevents a user or role from stopping activity streams.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DenyStopActivityStreams",  
            "Effect": "Deny",  
            "Action": "rds:StopActivityStream",  
            "Resource": "*"  
        }  
    ]  
}
```

]
}

Working with Amazon RDS Custom

Amazon RDS Custom automates database administration tasks and operations. RDS Custom makes it possible for you as a database administrator to access and customize your database environment and operating system. With RDS Custom, you can customize to meet the requirements of legacy, custom, and packaged applications.

The following video is an overview of Amazon RDS Custom from AWS re:Invent 2021.

Topics

- [Addressing the challenge of database customization \(p. 755\)](#)
- [Management model and benefits for Amazon RDS Custom \(p. 756\)](#)
- [Amazon RDS Custom architecture \(p. 758\)](#)
- [Security considerations for Amazon RDS Custom \(p. 762\)](#)
- [Working with RDS Custom for Oracle \(p. 763\)](#)
- [Working with RDS Custom for SQL Server \(p. 843\)](#)
- [Troubleshooting DB issues for Amazon RDS Custom \(p. 889\)](#)

Addressing the challenge of database customization

Amazon RDS Custom brings the benefits of Amazon RDS to a market that can't easily move to a fully managed service because of customizations that are required with third-party applications. Amazon RDS Custom saves administrative time, is durable, and scales with your business.

If you need the entire database and operating system to be fully managed by AWS, we recommend Amazon RDS. If you need administrative rights to the database and underlying operating system to make dependent applications available, Amazon RDS Custom is the better choice. If you want full management responsibility and simply need a managed compute service, the best option is self-managing your commercial databases on Amazon EC2.

To deliver a managed service experience, Amazon RDS doesn't let you access the underlying host. Amazon RDS also restricts access to some procedures and objects that require high-level privileges. However, for some applications, you might need to perform operations as a privileged operating system (OS) user.

For example, you might need to do the following:

- Install custom database and OS patches and packages.
- Configure specific database settings.
- Configure file systems to share files directly with their applications.

Previously, if you needed to customize your application, you had to deploy your database on-premises or on Amazon EC2. In this case, you bear most or all of the responsibility for database management, as summarized in the following table.

Feature	On-premises responsibility	Amazon EC2 responsibility	Amazon RDS responsibility
Application optimization	Customer	Customer	Customer
Scaling	Customer	Customer	AWS
High availability	Customer	Customer	AWS
Database backups	Customer	Customer	AWS
Database software patching	Customer	Customer	AWS
Database software install	Customer	Customer	AWS
OS patching	Customer	Customer	AWS
OS installation	Customer	Customer	AWS
Server maintenance	Customer	AWS	AWS
Hardware lifecycle	Customer	AWS	AWS
Power, network, and cooling	Customer	AWS	AWS

When you manage database software yourself, you gain more control, but you're also more prone to user errors. For example, when you make changes manually, you might accidentally cause application downtime. You might spend hours checking every change to identify and fix an issue. Ideally, you want a managed database service that automates common DBA tasks, but also supports privileged access to the database and underlying operating system.

Management model and benefits for Amazon RDS Custom

Amazon RDS Custom is a managed database service for legacy, custom, and packaged applications that require access to the underlying operating system and database environment. Amazon RDS Custom automates setup, operation, and scaling of databases in the AWS Cloud while granting you access to the database and underlying operating system. With this access, you can configure settings, install patches, and enable native features to meet the dependent application's requirements. With RDS Custom, you can run your database workload using the AWS Management Console or the AWS CLI.

Currently, Amazon RDS Custom supports only the Oracle Database and Microsoft SQL Server engines.

Shared responsibility model

With Amazon RDS Custom, you get the automation of Amazon RDS and the flexibility of Amazon EC2. You take on additional database management responsibilities beyond what you do in Amazon RDS. By doing so, you can benefit from RDS automation and the deeper customization of EC2. To meet your application and business requirements, you manage the host yourself.

In the shared responsibility model of RDS Custom, you get more control than in Amazon RDS but also more responsibility. Shared responsibility has two meanings:

1. You own part of the process when using a feature.
2. You have full access to the feature, and it's your responsibility to make sure that any customizations work with that feature.

The following table details the shared responsibility model for RDS Custom.

Feature	Amazon EC2 responsibility	Amazon RDS responsibility	RDS Custom for Oracle responsibility	RDS Custom for SQL Server responsibility
Application optimization	Customer	Customer	Customer	Customer
Scaling	Customer	AWS	Shared	Shared
High availability	Customer	AWS	Customer	Customer
Database backups	Customer	AWS	Shared	Shared
Database software patching	Customer	AWS	Shared	AWS
Database software install	Customer	AWS	Shared	AWS
OS patching	Customer	AWS	Customer	AWS
OS installation	Customer	AWS	Shared	AWS
Server maintenance	AWS	AWS	AWS	AWS
Hardware lifecycle	AWS	AWS	AWS	AWS
Power, network, and cooling	AWS	AWS	AWS	AWS

You can create an RDS Custom DB instance using Microsoft SQL Server. In this case:

- You don't manage your own media.
- You don't need to purchase SQL Server licenses separately. AWS holds the license for the SQL Server database software.

You can create an RDS Custom DB instance using Oracle Database. In this case, you do the following:

- Manage your own media.

When using RDS Custom, you upload your own database installation files and patches. You create a custom engine version (CEV) from these files. Then you can create an RDS Custom DB instance by using this CEV.

- Manage your own licenses.

You bring your own Oracle Database licenses and manage licenses by yourself.

Key benefits of RDS Custom

With RDS Custom, you can do the following:

- Automate many of the same administrative tasks as Amazon RDS, including the following:
 - Lifecycle management of databases
 - Automated backups and point-in-time recovery (PITR)
 - Monitoring the health of RDS Custom DB instances and observing changes to the infrastructure, operating system, and databases
 - Notification or taking action to fix issues depending on disruption to the DB instance
- Install third-party applications.

You can install software to run custom applications and agents. Because you have privileged access to the host, you can modify file systems to support legacy applications.

- Install custom patches.

You can apply custom database patches or modify OS packages on your RDS Custom DB instances.

- Stage an on-premises database before moving it to a fully managed service.

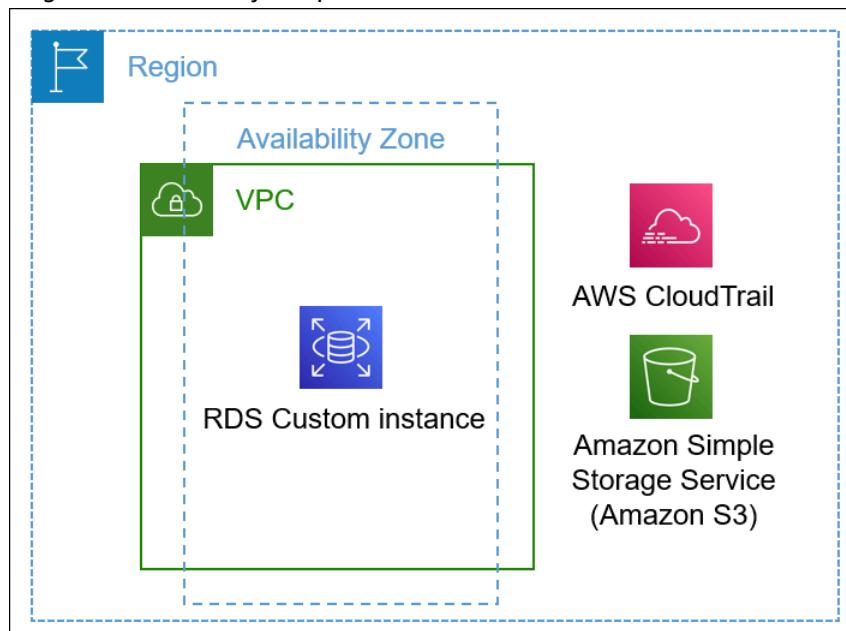
If you manage your own on-premises database, you can stage the database to RDS Custom as-is. After you familiarize yourself with the cloud environment, you can migrate your database to a fully managed Amazon RDS DB instance.

- Create your own automation.

You can create, schedule, and run custom automation scripts for reporting, management, or diagnostic tools.

Amazon RDS Custom architecture

Amazon RDS Custom architecture is based on Amazon RDS, with important differences. The following diagram shows the key components of the RDS Custom architecture.

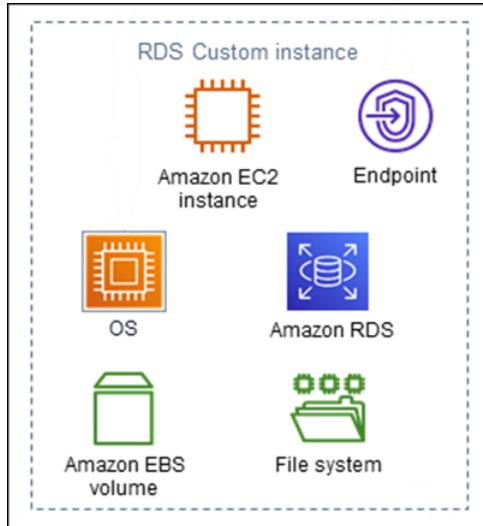


Topics

- [VPC \(p. 759\)](#)
- [Amazon S3 \(p. 759\)](#)
- [AWS CloudTrail \(p. 760\)](#)
- [RDS Custom automation and monitoring \(p. 760\)](#)

VPC

As in Amazon RDS, your RDS Custom DB instance resides in a virtual private cloud (VPC).



The DB instance consists of the following main components:

- Amazon EC2 instance
- Instance endpoint
- Operating system installed on the Amazon EC2 instance
- Amazon EBS storage, which contains any additional file systems

Amazon S3

If you use RDS Custom for Oracle, you upload installation media to a user-created Amazon S3 bucket. RDS Custom for Oracle uses the media in this bucket to create a custom engine version (CEV). A CEV is a binary volume snapshot of a database version and Amazon Machine Image (AMI). From the CEV, you can create an RDS Custom DB instance. For more information, see [Working with custom engine versions for Amazon RDS Custom for Oracle \(p. 781\)](#).

For both RDS Custom for Oracle and RDS Custom for SQL Server, RDS Custom automatically creates an Amazon S3 bucket prefixed with the string `do-not-delete-rds-custom-`. RDS Custom uses the `do-not-delete-rds-custom-` S3 bucket to store the following types of files:

- AWS CloudTrail logs for the trail created by RDS Custom
- Support perimeter artifacts (see [Support perimeter \(p. 761\)](#))
- Database redo log files (RDS Custom for Oracle only)
- Transaction logs (RDS Custom for SQL Server only)
- Custom engine version artifacts (RDS Custom for Oracle only)

RDS Custom creates the do-not-delete-rds-custom- S3 bucket when you create either of the following resources:

- Your first CEV for RDS Custom for Oracle
- Your first DB instance for RDS Custom for SQL Server

RDS Custom creates one bucket for each combination of the following:

- AWS account ID
- Engine type (either RDS Custom for Oracle or RDS Custom for SQL Server)
- AWS Region

For example, if you create RDS Custom for Oracle CEVs in a single AWS Region, one do-not-delete-rds-custom- bucket exists. If you create multiple RDS Custom for SQL Server instances, and they reside in different AWS Regions, one do-not-delete-rds-custom- bucket exists in each AWS Region. If you create one RDS Custom for Oracle instance and two RDS Custom for SQL Server instances in a single AWS Region, two do-not-delete-rds-custom- buckets exist.

AWS CloudTrail

RDS Custom automatically creates an AWS CloudTrail trail whose name begins with do-not-delete-rds-custom-. The RDS Custom support perimeter relies on the events from CloudTrail to determine whether your actions affect RDS Custom automation. For more information, see [Support perimeter \(p. 761\)](#).

RDS Custom creates the trail when you create your first DB instance. RDS Custom creates one trail for each combination of the following:

- AWS account ID
- Engine type (either RDS Custom for Oracle or RDS Custom for SQL Server)
- AWS Region

RDS Custom automation and monitoring

RDS Custom has automation software that runs outside of the DB instance. This software communicates with agents on the DB instance and with other components within the overall RDS Custom environment.

Monitoring and recovery

The RDS Custom monitoring and recovery features offer similar functionality to Amazon RDS. By default, RDS Custom is in full automation mode. The automation software has the following primary responsibilities:

- Collect metrics and send notifications
- Perform automatic instance recovery

An important responsibility of RDS Custom automation is responding to problems with your Amazon EC2 instance. For various reasons, the host might become impaired or unreachable. RDS Custom resolves these problems by either rebooting or replacing the Amazon EC2 instance.

The automated replacement preserves all database data. On RDS Custom for SQL Server, host replacement doesn't preserve operating system customizations or data on the C: drive.

The only customer-visible change when a host is replaced is a new public IP address. For more information, see [How Amazon RDS Custom replaces an impaired host \(p. 897\)](#).

Support perimeter

RDS Custom provides additional monitoring capability called the *support perimeter*. This additional monitoring ensures that your RDS Custom instance uses a supported AWS infrastructure, operating system, and database. For more information about the support perimeter, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

Security considerations for Amazon RDS Custom

When you create an Amazon RDS Custom for Oracle custom engine version (CEV) or an RDS Custom for SQL Server DB instance, RDS Custom creates an Amazon S3 bucket. The S3 bucket stores files such as CEV artifacts, redo (transaction) logs, configuration items for the support perimeter, and AWS CloudTrail logs.

You can make these S3 buckets more secure by using the global condition context keys to prevent the *confused deputy problem*. For more information, see [Preventing cross-service confused deputy problems \(p. 2046\)](#).

The following RDS Custom for Oracle example shows the use of the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in an S3 bucket policy. For RDS Custom for Oracle, make sure to include the Amazon Resource Names (ARNs) for the CEVs and the DB instances. For RDS Custom for SQL Server, make sure to include the ARN for the DB instances.

```
...
{
    "Sid": "AWSRDSCustomForOracleInstancesObjectLevelAccess",
    "Effect": "Allow",
    "Principal": {
        "Service": "custom.rds.amazonaws.com"
    },
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectRetention",
        "s3:BypassGovernanceRetention"
    ],
    "Resource": "arn:aws:s3:::do-not-delete-rds-custom-123456789012-us-east-2-c8a6f7/RDSCustomForOracle/Instances/*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": [
                "arn:aws:rds:us-east-2:123456789012:db:/*",
                "arn:aws:rds:us-east-2:123456789012:cev:/*"
            ]
        },
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        }
    }
}, ...
}
```

Working with RDS Custom for Oracle

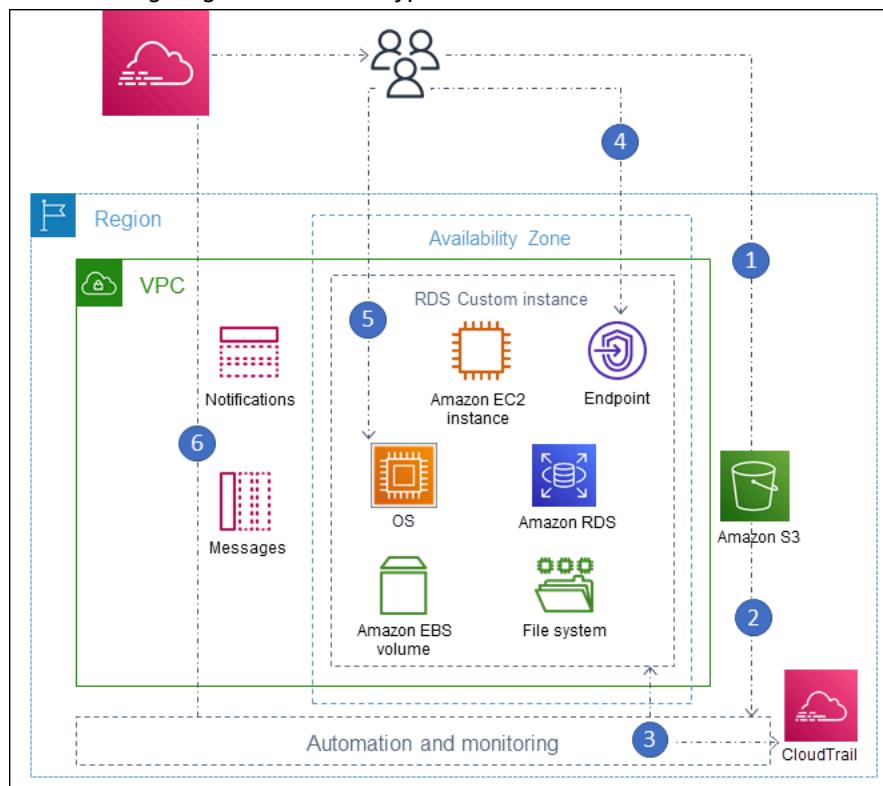
Following, you can find instructions for creating, managing, and maintaining your RDS Custom for Oracle DB instances.

Topics

- [RDS Custom for Oracle workflow \(p. 763\)](#)
- [Availability and requirements for Amazon RDS Custom for Oracle \(p. 766\)](#)
- [Setting up your environment for Amazon RDS Custom for Oracle \(p. 768\)](#)
- [Working with custom engine versions for Amazon RDS Custom for Oracle \(p. 781\)](#)
- [Configuring a DB instance for Amazon RDS Custom for Oracle \(p. 807\)](#)
- [Managing an Amazon RDS Custom for Oracle DB instance \(p. 816\)](#)
- [Working with Oracle replicas for RDS Custom for Oracle \(p. 826\)](#)
- [Backing up and restoring an Amazon RDS Custom for Oracle DB instance \(p. 831\)](#)
- [Upgrading a DB instance for Amazon RDS Custom for Oracle \(p. 838\)](#)

RDS Custom for Oracle workflow

The following diagram shows the typical workflow for RDS Custom for Oracle.



The steps are as follows:

1. Upload your database software to your Amazon S3 bucket.

For more information, see [Uploading your installation files to Amazon S3 \(p. 786\)](#).

2. Create an RDS Custom custom engine version (CEV) from your media.

For more information, see [Creating a CEV \(p. 798\)](#).

3. Create an RDS Custom DB instance from a CEV.

For more information, see [Creating an RDS Custom for Oracle DB instance \(p. 808\)](#).

4. Connect your application to the RDS Custom DB instance endpoint.

For more information, see [Connecting to your RDS Custom DB instance using SSH \(p. 812\)](#) and [Connecting to your RDS Custom DB instance using AWS Systems Manager \(p. 814\)](#).

5. (Optional) Access the host to customize your software.

6. Monitor notifications and messages generated by RDS Custom automation.

Database installation files

Your responsibility for media is a key difference between Amazon RDS and RDS Custom. Amazon RDS, which is a fully managed service, supplies the Amazon Machine Image (AMI) and database software. The Amazon RDS database software is preinstalled, so you need only choose a database engine and version, and create your database.

For RDS Custom, you supply your own media. When you create a custom engine version, RDS Custom installs the media that you provide. RDS Custom media contains your database installation files and patches. This service model is called *Bring Your Own Media (BYOM)*.

Custom engine version

An *RDS Custom custom engine version (CEV)* is a binary volume snapshot of a database version and AMI. You store your database installation files in Amazon S3. When you create your CEV, you specify the files in a JSON document called a *CEV manifest*. You can also specify installation parameters that set nondefault values for the Oracle base, Oracle home, and the ID and name of the UNIX/Linux user and group.

Name your CEV using a customer-specified string. The name format is the following, depending on your Oracle Database release:

- 19.*customized_string*
- 18.*customized_string*
- 12.2.*customized_string*
- 12.1.*customized_string*

You can use 1–50 alphanumeric characters, underscores, dashes, and periods. For example, you might name your CEV 19.my_cev1. When you create a CEV, you can specify the Oracle Multitenant option. You can create container databases (CDBs) only when the CEV was created with the Oracle Multitenant option. For more information, see [Working with custom engine versions for Amazon RDS Custom for Oracle \(p. 781\)](#).

Creating a DB instance for RDS Custom for Oracle

After you create your CEV, it's available for use. You can create multiple CEVs, and you can create multiple RDS Custom for Oracle DB instances from any CEV. You can also change the status of a CEV to make it available or inactive.

You can either create your RDS Custom for Oracle DB instance with the Oracle Multitenant architecture (custom-oracle-ee-cdb engine type) or with the traditional non-CDB architecture (custom-oracle-ee engine type). When you create a container database (CDB), it contains one pluggable database (PDB) and one PDB seed. You can create additional PDBs manually using Oracle SQL.

To create your RDS Custom for Oracle DB instance, use the `create-db-instance` command. In this command, specify which CEV to use. The procedure is similar to creating an Amazon RDS DB instance. However, some parameters are different. For more information, see [Configuring a DB instance for Amazon RDS Custom for Oracle \(p. 807\)](#).

Database connection

Like an Amazon RDS DB instance, an RDS Custom DB instance resides in a virtual private cloud (VPC). Your application connects to the Oracle database using an Oracle listener.

If your database is a CDB, you can use the listener `L_RDSCDB_001` to connect to the CDB root and to a PDB. If you plug a non-CDB into a CDB, make sure to set `USE_SID_AS_SERVICE_LISTENER = ON` so that migrated applications keep the same settings.

When you connect to a non-CDB, the master user is the user for the non-CDB. When you connect to a CDB, the master user is the user for the PDB. To connect to the CDB root, log in to the host, start a SQL client, and create an administrative user with SQL commands.

RDS Custom customization

You can access the RDS Custom host to install or customize software. To avoid conflicts between your changes and the RDS Custom automation, you can pause the automation for a specified period. During this period, RDS Custom doesn't perform monitoring or instance recovery. At the end of the period, RDS Custom resumes full automation. For more information, see [Pausing and resuming RDS Custom automation \(p. 817\)](#).

Availability and requirements for Amazon RDS Custom for Oracle

In this topic, you can find a summary of the Amazon RDS Custom for Oracle feature availability and requirements for quick reference.

Topics

- [Region and version availability \(p. 766\)](#)
- [DB instance class support for RDS Custom for Oracle \(p. 766\)](#)
- [General requirements for RDS Custom for Oracle \(p. 766\)](#)
- [Limitations for RDS Custom for Oracle \(p. 766\)](#)

Region and version availability

Feature availability and support vary across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of Amazon RDS Custom for Oracle, see [RDS Custom \(p. 110\)](#).

DB instance class support for RDS Custom for Oracle

RDS Custom for Oracle supports the following DB instance classes:

- db.m5.large–db.m5.24xlarge
- db.r5.large–db.r5.24xlarge

General requirements for RDS Custom for Oracle

Make sure to follow these requirements for Amazon RDS Custom for Oracle:

- Use [Oracle Software Delivery Cloud](#) to download Oracle installation and patch files. For more information, see [Prerequisites for creating an RDS Custom for Oracle instance \(p. 768\)](#).
- Use the DB instance classes shown in [DB instance class support for RDS Custom for Oracle \(p. 766\)](#). The instances must run Oracle Linux 7 Update 6. The only storage types supported are solid state drives (SSD) of types gp2 and io1. The maximum storage limit is 64 TiB.
- Make sure that you have an AWS KMS key to create an RDS Custom DB instance. For more information, see [Make sure that you have a symmetric encryption AWS KMS key \(p. 768\)](#).
- Use only the approved database installation and patch files. For more information, see [Downloading your database installation files and patches from Oracle Software Delivery Cloud \(p. 781\)](#).
- Create an AWS Identity and Access Management (IAM) role and instance profile. For more information, see [Configuring IAM and your VPC \(p. 769\)](#).
- Make sure to supply a networking configuration that RDS Custom can use to access other AWS services. For specific requirements, see [Configuring IAM and your VPC \(p. 769\)](#).
- Make sure that the combined number of RDS Custom and Amazon RDS DB instances doesn't exceed your quota limit. For example, if your quota for Amazon RDS is 40 DB instances, you can have 20 RDS Custom for Oracle DB instances and 20 Amazon RDS DB instances.

Limitations for RDS Custom for Oracle

The following limitations apply to RDS Custom for Oracle:

- You can't provide your own AMI.
- Not all options are supported. For example, when you create or modify an RDS Custom for Oracle DB instance, you can't do the following:
 - Change the number of CPU cores and threads per core on the DB instance class.
 - Turn on storage autoscaling.
 - Set backup retention to 0.
 - Configure Kerberos authentication.
 - Specify your own DB parameter group or option group.
 - Turn on Performance Insights.
 - Turn on automatic minor version upgrade.
- Change the DB instance class. For example, you can't change a db.m5.xlarge DB instance to db.m5.2xlarge. However, you can restore a snapshot of your RDS Custom for Oracle DB instance to a different instance class.
- The maximum DB instance storage is 64 TiB.
- Only one database is supported on an RDS Custom for Oracle DB instance.

Setting up your environment for Amazon RDS Custom for Oracle

Before you create a DB instance based on Amazon RDS Custom for Oracle, perform the following tasks.

Topics

- [Prerequisites for creating an RDS Custom for Oracle instance \(p. 768\)](#)
- [Make sure that you have a symmetric encryption AWS KMS key \(p. 768\)](#)
- [Download and install the AWS CLI \(p. 769\)](#)
- [Configuring IAM and your VPC \(p. 769\)](#)
- [Grant required permissions to your IAM user \(p. 778\)](#)

Prerequisites for creating an RDS Custom for Oracle instance

Before creating an RDS Custom for Oracle DB instance, make sure that you meet the following prerequisites:

- You have access to [My Oracle Support](#) and [Oracle Software Delivery Cloud](#) to download the supported list of installation files and patches for the Enterprise Edition of any of the following Oracle Database releases:
 - Oracle Database 19c
 - Oracle Database 18c
 - Oracle Database 12c Release 2 (12.2)
 - Oracle Database 12c Release 1 (12.1)

If you use an unknown patch, custom engine version (CEV) creation fails. In this case, contact the RDS Custom support team and ask it to add the missing patch.

For more information, see [Downloading your database installation files and patches from Oracle Software Delivery Cloud \(p. 781\)](#).

- You have access to Amazon S3 so that you can upload your Oracle installation files. You use the installation files when you create your RDS Custom CEV.

For more information, see [Uploading your installation files to Amazon S3 \(p. 786\)](#) and [Creating a CEV \(p. 798\)](#).

- You supply your own virtual private cloud (VPC) and security group configuration. For more information, see [Configuring IAM and your VPC \(p. 769\)](#).
- The AWS Identity and Access Management (IAM) user that creates a CEV or RDS Custom DB instance has the required permissions for IAM, CloudTrail, and Amazon S3.

For more information, see [Grant required permissions to your IAM user \(p. 778\)](#).

For each task, the following sections describe the requirements and limitations specific to the task. For example, when you create your RDS Custom DB for Oracle instance, use either the db.m5 or db.r5 instance classes running Oracle Linux 7 Update 6. For general requirements that apply to RDS Custom, see [Availability and requirements for Amazon RDS Custom for Oracle \(p. 766\)](#).

Make sure that you have a symmetric encryption AWS KMS key

A symmetric encryption AWS KMS key is required for RDS Custom. When you create an RDS Custom for Oracle DB instance, you supply the KMS key identifier. For more information, see [Configuring a DB instance for Amazon RDS Custom for Oracle \(p. 807\)](#).

You have the following options:

- If you have an existing KMS key in your AWS account, you can use it with RDS Custom. No further action is necessary.
- If you already created a symmetric encryption KMS key for a different RDS Custom engine, you can reuse the same KMS key. No further action is necessary.
- If you don't have an existing symmetric encryption KMS key in your account, create a KMS key by following the instructions in [Creating keys](#) in the *AWS Key Management Service Developer Guide*.
- If you're creating a CEV or RDS Custom DB instance, and your KMS key is in a different AWS account, make sure to use the AWS CLI. You can't use the AWS console with cross-account KMS keys.

RDS Custom doesn't support AWS-managed KMS keys.

Make sure that the symmetric encryption key that you use gives the AWS Identity and Access Management (IAM) role in your IAM instance profile access to the kms : Decrypt and kms : GenerateDataKey operations. If you have a new symmetric encryption key in your account, no changes are required. Otherwise, make sure that your symmetric encryption key's policy can give access to these operations.

For more information about configuring IAM for RDS Custom for Oracle, see [Configuring IAM and your VPC \(p. 769\)](#).

Download and install the AWS CLI

AWS provides you with a command-line interface to use RDS Custom features. You can use either version 1 or version 2 of the AWS CLI.

For information about downloading and installing the AWS CLI, see [Installing or updating the latest version of the AWS CLI](#).

If you plan to access RDS Custom only from the AWS Management Console, skip this step.

If you have already downloaded the AWS CLI for Amazon RDS or a different RDS Custom engine, skip this step.

Configuring IAM and your VPC

You can configure your IAM role and virtual private cloud (VPC) using either of the following techniques:

- [Configuring IAM and your VPC using AWS CloudFormation \(p. 769\)](#) (recommended)
- Following the procedures in [Creating your IAM role and instance profile manually \(p. 770\)](#) and [Configuring your VPC manually \(p. 774\)](#)

Configuring IAM and your VPC using AWS CloudFormation

To simplify setup, you can use the AWS CloudFormation template files to create CloudFormation stacks. To learn how to create stacks, see [Creating a stack on the AWS CloudFormation console](#) in *AWS CloudFormation User Guide*.

To download the template files

1. Open the context (right-click) menu for the link [custom-oracle-iam.zip](#) and choose **Save Link As**.
2. Save the file to your computer.
3. Repeat the previous steps for the link [custom-vpc.zip](#).

If you already configured your VPC for RDS Custom for SQL Server, skip this step.

To configure IAM using CloudFormation

1. Open the CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
2. Start the Create Stack wizard, and choose **Create Stack**.
3. On the **Specify template** page, do the following:
 - a. For **Template source**, choose **Upload a template file**.
 - b. For **Choose file**, navigate to, then choose `custom-oracle-iam.json`.
 - c. Choose **Next**.
4. On the **Specify stack details** page, do the following:
 - a. For **Stack name**, enter `custom-oracle-iam`.
 - b. Choose **Next**.
5. On the **Configure stack options** page, choose **Next**.
6. On the **Review custom-oracle-iam** page, do the following:
 - a. For **Capabilities**, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** check box.
 - b. Choose **Create stack**.

CloudFormation creates the IAM roles that RDS Custom for Oracle requires.

To configure your VPC using CloudFormation

This procedure assumes that you've already used CloudFormation to create your IAM roles.

If you've already configured your VPC for a different RDS Custom engine, skip this step.

1. Open the CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
2. On the **Stacks** page, for **Create stack** choose **With new resources (standard)**.
3. On the **Specify template** page, do the following:
 - a. For **Template source**, choose **Upload a template file**.
 - b. For **Choose file**, go to and choose `custom-vpc.json`.
 - c. Choose **Next**.
4. On the **Specify stack details** page, do the following:
 - a. For **Stack name**, enter `custom-vpc`.
 - b. For **Parameters**, choose the private subnets to use for RDS Custom DB instances.
 - c. Choose the private VPC ID to use for RDS Custom DB instances.
 - d. Enter the route table associated with the private subnets.
 - e. Choose **Next**.
5. On the **Configure stack options** page, choose **Next**.
6. On the **Review custom-vpc** page, choose **Create stack**.

CloudFormation configures your VPC.

Creating your IAM role and instance profile manually

To use RDS Custom, you create an IAM instance profile named `AWSRDSCustomInstanceProfileForRdsCustomInstance`. You also create the IAM role

AWSRDSCustomInstanceRoleForRdsCustomInstance for the instance profile. You then add AWSRDSCustomInstanceRoleForRdsCustomInstance to your instance profile.

The following section explains how to perform the task without using CloudFormation.

To create the RDS Custom instance profile and add the necessary role to it

1. Create the IAM role named AWSRDSCustomInstanceRoleForRdsCustomInstance with a trust policy that Amazon EC2 can use to assume this role.
2. Add an access policy to AWSRDSCustomInstanceRoleForRdsCustomInstance.
3. Create an IAM instance profile for RDS Custom named AWSRDSCustomInstanceProfileForRdsCustomInstance.
4. Add the AWSRDSCustomInstanceRoleForRdsCustomInstance IAM role to the instance profile.

Create the role AWSRDSCustomInstanceRoleForRdsCustomInstance

The following example creates the role AWSRDSCustomInstanceRoleForRdsCustomInstance. Using the trust policy, Amazon EC2 can assume the role.

```
aws iam create-role \
--role-name AWSRDSCustomInstanceRoleForRdsCustomInstance \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
        }
    ]
}'
```

Add an access policy to AWSRDSCustomInstanceRoleForRdsCustomInstance

When you embed an inline policy in an IAM role, the inline policy is used as part of the role's access (permissions) policy. You create the AWSRDSCustomIamRolePolicy policy that permits Amazon EC2 to send and receive messages and perform various actions.

The following example creates the access policy named AWSRDSCustomIamRolePolicy, and adds it to the IAM role AWSRDSCustomInstanceRoleForRdsCustomInstance. This example assumes that you have set the \$REGION and \$ACCOUNT_ID variables in the AWS CLI. This example also requires the Amazon Resource Name (ARN) of the AWS KMS key that you want to use for your RDS Custom DB instances.

To specify more than one KMS key, add it to the Resources section of statement ID (Sid) 11.

```
aws iam put-role-policy \
--role-name AWSRDSCustomInstanceRoleForRdsCustomInstance \
--policy-name AWSRDSCustomIamRolePolicy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:PutAssociationResult"
            ],
            "Resource": [
                "arn:aws:kms:$REGION:$ACCOUNT_ID/*"
            ]
        }
    ]
}'
```

```
    "ssm:GetDeployablePatchSnapshotForInstance",
    "ssm:GetDocument",
    "ssm:DescribeDocument",
    "ssm:GetManifest",
    "ssm:GetParameter",
    "ssm:GetParameters",
    "ssm>ListAssociations",
    "ssm>ListInstanceAssociations",
    "ssm:PutInventory",
    "ssm:PutComplianceItems",
    "ssm:PutConfigurePackageResult",
    "ssm:UpdateAssociationStatus",
    "ssm:UpdateInstanceAssociationStatus",
    "ssm:UpdateInstanceInformation",
    "ssm:GetConnectionStatus",
    "ssm:DescribeInstanceInformation",
    "ssmmessages>CreateControlChannel",
    "ssmmessages>CreateDataChannel",
    "ssmmessages:OpenControlChannel",
    "ssmmessages:OpenDataChannel"
],
"Resource": [
    "*"
]
},
{
    "Sid": "2",
    "Effect": "Allow",
    "Action": [
        "ec2messages:AcknowledgeMessage",
        "ec2messages>DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "3",
    "Effect": "Allow",
    "Action": [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs>CreateLogStream",
        "logs>CreateLogGroup"
    ],
    "Resource": [
        "arn:aws:logs:$REGION*:log-group:rds-custom-instance*"
    ]
},
{
    "Sid": "4",
    "Effect": "Allow",
    "Action": [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
    ]
}
```

```

        },
        {
            "Sid": "5",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "RDSCustomForOracle/Agent"
                    ]
                }
            }
        },
        {
            "Sid": "6",
            "Effect": "Allow",
            "Action": [
                "events:PutEvents"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "7",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:'$REGION':'$ACCOUNT_ID':secret:do-not-delete-rds-
custom-*"
            ]
        },
        {
            "Sid": "8",
            "Effect": "Allow",
            "Action": [
                "s3>ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::do-not-delete-rds-custom-*"
            ]
        },
        {
            "Sid": "9",
            "Effect": "Allow",
            "Action": "ec2>CreateSnapshots",
            "Resource": [
                "arn:aws:ec2:*.*:instance/*",
                "arn:aws:ec2:*.*:volume/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSRDSCustom": "custom-oracle"
                }
            }
        },
        {
            "Sid": "10",

```

```

        "Effect": "Allow",
        "Action": "ec2:CreateSnapshots",
        "Resource": [
            "arn:aws:ec2:*::snapshot/*"
        ]
    },
    {
        "Sid": "11",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": [
            "arn:aws:kms:'$REGION':'$ACCOUNT_ID':key/abcd1234-5678-eeff-9012-123456abcdef"
        ]
    },
    {
        "Sid": "12",
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ec2:CreateAction": [
                    "CreateSnapshots"
                ]
            }
        }
    }
]
}

```

Create your RDS Custom instance profile

Create your IAM instance profile as follows, naming it `AWSRDSCustomInstanceProfileForRdsCustomInstance`.

```
aws iam create-instance-profile \
--instance-profile-name AWSRDSCustomInstanceProfileForRdsCustomInstance
```

Add `AWSRDSCustomInstanceRoleForRdsCustomInstance` to your RDS Custom instance profile

Add the IAM role `AWSRDSCustomInstanceRoleForRdsCustomInstance` to the profile `AWSRDSCustomInstanceProfileForRdsCustomInstance`.

```
aws iam add-role-to-instance-profile \
--instance-profile-name AWSRDSCustomInstanceProfileForRdsCustomInstance \
--role-name AWSRDSCustomInstanceRoleForRdsCustomInstance
```

Configuring your VPC manually

Your RDS Custom DB instance is in a virtual private cloud (VPC) based on the Amazon VPC service, just like an Amazon EC2 instance or Amazon RDS instance. You provide and configure your own VPC. Thus, you have full control over your instance networking setup.

RDS Custom sends communication from your DB instance to other AWS services. To make sure that RDS Custom can communicate, it validates network connectivity to these services.

Your DB instance communicates with the following AWS services:

- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CloudWatch Events
- Amazon EC2
- Amazon EventBridge
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Make sure that VPC components involved in communication between the DB instance and AWS services are configured with the following requirements:

- The DB instance can make outbound connections on port 443 to other AWS services.
- The VPC allows incoming responses to requests originating from your DB instance.
- Correctly resolve the domain names of endpoints for each AWS service.

If you already configured a VPC for a different RDS Custom engine, you can reuse that VPC and skip this process.

Topics

- [Configure your instance security group \(p. 775\)](#)
- [Configure endpoints for dependent AWS services \(p. 776\)](#)
- [Configure the instance metadata service \(p. 777\)](#)

Configure your instance security group

A *security group* acts as a virtual firewall for a VPC instance, controlling both inbound and outbound traffic. An RDS Custom DB instance has a default security group that protects the instance. Make sure that your security group permits traffic between RDS Custom and other AWS services.

To configure your security group for RDS Custom

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc>.
2. Allow RDS Custom to use the default security group, or create your own security group.

For detailed instructions, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

3. Make sure that your security group permits outbound connections on port 443. RDS Custom needs this port to communicate with dependent AWS services.
4. If you have a private VPC and use VPC endpoints, make sure that the security group associated with the DB instance allows outbound connections on port 443 to VPC endpoints. Also make sure that the security group associated with the VPC endpoint allows inbound connections on port 443 from the DB instance.

If incoming connections aren't allowed, the RDS Custom instance can't connect to the AWS Systems Manager and Amazon EC2 endpoints. For more information, see [Create a Virtual Private Cloud endpoint](#) in the *AWS Systems Manager User Guide*.

For more information about security groups, see [Security groups for your VPC](#) in the *Amazon VPC Developer Guide*.

Configure endpoints for dependent AWS services

Make sure that your VPC allows outbound traffic to the following AWS services with which the DB instance communicates:

- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CloudWatch Events
- Amazon EC2
- Amazon EventBridge
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

We recommend that you add endpoints for every service to your VPC using the following instructions. However, you can use any solution that lets your VPC communicate with AWS service endpoints. For example, you can use Network Address Translation (NAT) or AWS Direct Connect.

To configure endpoints for AWS services with which RDS Custom works

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. On the navigation bar, use the Region selector to choose the AWS Region.
3. In the navigation pane, choose **Endpoints**. In the main pane, choose **Create Endpoint**.
4. For **Service category**, choose **AWS services**.
5. For **Service Name**, choose the endpoint shown in the table.
6. For **VPC**, choose your VPC.
7. For **Subnets**, choose a subnet from each Availability Zone to include.

The VPC endpoint can span multiple Availability Zones. AWS creates an elastic network interface for the VPC endpoint in each subnet that you choose. Each network interface has a Domain Name System (DNS) host name and a private IP address.

8. For **Security group**, choose or create a security group.

You can use security groups to control access to your endpoint, much as you use a firewall. For more information about security groups, see [Security groups for your VPC](#) in the *Amazon VPC User Guide*.

9. Optionally, you can attach a policy to the VPC endpoint. Endpoint policies can control access to the AWS service to which you are connecting. The default policy allows all requests to pass through the endpoint. If you're using a custom policy, make sure that requests from the DB instance are allowed in the policy.
10. Choose **Create endpoint**.

The following table explains how to find the list of endpoints that your VPC needs for outbound communications.

Service	Endpoint format	Notes and links
AWS Systems Manager	Use the following endpoint formats: <ul style="list-style-type: none">• <code>ssm.region.amazonaws.com</code>• <code>ssmmessages.region.amazonaws.com</code>	For the list of endpoints in each Region, see AWS Systems Manager endpoints and quotas in the <i>Amazon Web Services General Reference</i> .

Service	Endpoint format	Notes and links
AWS Secrets Manager	Use the endpoint format <code>secretsmanager.region.amazonaws.com</code> .	For the list of endpoints in each Region, see AWS Secrets Manager endpoints and quotas in the <i>Amazon Web Services General Reference</i> .
Amazon CloudWatch	Use the following endpoint formats: <ul style="list-style-type: none"> For CloudWatch metrics, use <code>monitoring.region.amazonaws.com</code> For CloudWatch Events, use <code>events.region.amazonaws.com</code> For CloudWatch Logs, use <code>logs.region.amazonaws.com</code> 	For the list of endpoints in every Region, see: <ul style="list-style-type: none"> Amazon CloudWatch endpoints and quotas in the <i>Amazon Web Services General Reference</i> Amazon CloudWatch Logs endpoints and quotas in the <i>Amazon Web Services General Reference</i> Amazon CloudWatch Events endpoints and quotas in the <i>Amazon Web Services General Reference</i>
Amazon EC2	Use the following endpoint formats: <ul style="list-style-type: none"> <code>ec2.region.amazonaws.com</code> <code>ec2messages.region.amazonaws.com</code> 	For the list of endpoints in each Region, see Amazon Elastic Compute Cloud endpoints and quotas in the <i>Amazon Web Services General Reference</i> .
Amazon S3	Use the endpoint format <code>s3.region.amazonaws.com</code> .	For the list of endpoints in each Region, see Amazon Simple Storage Service endpoints and quotas in the <i>Amazon Web Services General Reference</i> . <p>To learn more about gateway endpoints for Amazon S3, see Endpoints for Amazon S3 in the <i>Amazon VPC Developer Guide</i>.</p> <p>To learn how to create an access point, see Creating access points in the <i>Amazon VPC Developer Guide</i>.</p> <p>To learn how to create a gateway endpoints for Amazon S3, see Gateway VPC endpoints.</p>

Configure the instance metadata service

Make sure that your instance can do the following:

- Access the instance metadata service using Instance Metadata Service Version 2 (IMDSv2).
- Allow outbound communications through port 80 (HTTP) to the IMDS link IP address.
- Request instance metadata from `http://169.254.169.254`, the IMDSv2 link.

For more information, see [Use IMDSv2](#) in the *Amazon EC2 User Guide for Linux Instances*.

RDS Custom for Oracle automation uses IMDSv2 by default, by setting `HttpTokens=enabled` on the underlying Amazon EC2 instance. However, you can use IMDSv1 if you want. For more information, see [Configure the instance metadata options](#) in the *Amazon EC2 User Guide for Linux Instances*.

Grant required permissions to your IAM user

Make sure that the IAM principal that creates the CEV or DB instance has either of the following policies:

- The `AdministratorAccess` policy
- The `AmazonRDSFullAccess` policy with required permissions for Amazon S3 and AWS KMS (required for both CEV and DB creation), CEV creation, and DB instance creation.

Topics

- [Permissions required for Amazon S3 and AWS KMS \(p. 778\)](#)
- [Permissions required for creating a CEV \(p. 778\)](#)
- [Permissions required for creating a DB instance from a CEV \(p. 779\)](#)

Permissions required for Amazon S3 and AWS KMS

To create CEVs or RDS Custom for Oracle DB instances, the IAM principal needs to access Amazon S3 and AWS KMS. The following sample JSON policy grants the required permissions.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "CreateS3Bucket",  
            "Effect": "Allow",  
            "Action": [  
                "s3:CreateBucket",  
                "s3:PutBucketPolicy",  
                "s3:PutBucketObjectLockConfiguration",  
                "s3:PutBucketVersioning"  
            ],  
            "Resource": "arn:aws:s3:::do-not-delete-rds-custom-*"  
        },  
        {  
            "Sid": "CreateKmsGrant",  
            "Effect": "Allow",  
            "Action": "kms>CreateGrant",  
            "Resource": "*"  
        }  
    ]  
}
```

For more information about the `kms>CreateGrant` permission, see [AWS KMS key management \(p. 2004\)](#).

Permissions required for creating a CEV

To create a CEV, the IAM principal needs the following additional permissions:

```
s3:GetObjectAcl  
s3:GetObject  
s3:GetObjectTagging  
s3>ListBucket  
mediaimport>CreateDatabaseBinarySnapshot
```

The following sample JSON policy grants the additional permissions to bucket `my-custom-installation-files` and its contents.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessToS3MediaBucket",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3>ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::my-custom-installation-files",
                "arn:aws:s3:::my-custom-installation-files/*"
            ]
        },
        {
            "Sid": "PermissionForByom",
            "Effect": "Allow",
            "Action": [
                "mediaimport>CreateDatabaseBinarySnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

You can grant similar permissions for Amazon S3 to caller accounts using an S3 bucket policy.

Permissions required for creating a DB instance from a CEV

To create a DB instance from an existing CEV, the IAM principal needs the following additional permissions:

```
iam:SimulatePrincipalPolicy
cloudtrail>CreateTrail
cloudtrail:StartLogging
```

The following sample JSON policy grants the required permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateIamRole",
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "*"
        },
        {
            "Sid": "CreateCloudTrail",
            "Effect": "Allow",
            "Action": [
                "cloudtrail>CreateTrail",
                "cloudtrail:StartLogging"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
        }
    ]
}
```


Working with custom engine versions for Amazon RDS Custom for Oracle

A *custom engine version (CEV)* for Amazon RDS Custom for Oracle is a binary volume snapshot of a database engine and specific Amazon Machine Image (AMI). You store your database installation files in Amazon S3. RDS Custom uses the installation files to create your CEV for you.

Topics

- [Preparing to create a CEV \(p. 781\)](#)
- [Creating a CEV \(p. 798\)](#)
- [Modifying CEV status \(p. 801\)](#)
- [Viewing CEV details \(p. 803\)](#)
- [Deleting a CEV \(p. 805\)](#)

Preparing to create a CEV

To create a CEV, access the installation files and patches that are stored in your Amazon S3 bucket for any of the following releases:

- Oracle Database 19c
- Oracle Database 18c
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1)

For example, you can use the April 2021 RU/RUR for Oracle Database 19c, or any valid combination of installation files and patches.

Topics

- [Downloading your database installation files and patches from Oracle Software Delivery Cloud \(p. 781\)](#)
- [Uploading your installation files to Amazon S3 \(p. 786\)](#)
- [Sharing your installation media in S3 across AWS accounts \(p. 787\)](#)
- [Preparing the CEV manifest \(p. 789\)](#)
- [Validating the CEV manifest \(p. 798\)](#)
- [Adding necessary IAM permissions \(p. 798\)](#)

Downloading your database installation files and patches from Oracle Software Delivery Cloud

The Oracle Database installation files and patches are hosted on Oracle Software Delivery Cloud.

To download the database installation files for Oracle Database 19c

1. Go to <https://edelivery.oracle.com/> and sign in.
2. In the box, enter **Oracle Database Enterprise Edition** and choose **Search**.
3. Choose **DLP: Oracle Database Enterprise Edition 19.3.0.0.0 (Oracle Database Enterprise Edition)**.
4. Choose **Continue**.
5. Clear the **Download Queue** check box.
6. Choose **Oracle Database 19.3.0.0.0 - Long Term Release**.

7. Choose **Linux x86-64** in **Platform/Languages**.
8. Choose **Continue**, and then sign the waiver.
9. Choose **V982063-01.zip**, choose **Download**, and then save the file.

Note

The SHA-256 hash is
BA8329C757133DA313ED3B6D7F86C5AC42CD9970A28BF2E6233F3235233AA8D8.

10. Click the links in the following table to download the Oracle patches. All URLs are for updates.oracle.com or support.oracle.com.

File	Description
p6880880_190000_Linux-x86-64.zip	OPatch for this version of Oracle
p32126828_190000_Linux-x86-64.zip	Patch 32126828 - COMBO OF OJVM RU COMPONENT 19.10.0.0.210119 + DB RU 19.10.0.0.210119
p29213893_1910000DBRU_Generic.zip	Patch 29213893: DBMS_STATS FAILING WITH ERROR ORA-01422 WHEN GATHERING STATS FOR USER TABLE
p29782284_1910000DBRU_Generic.zip	Patch 29782284: ORA-06508: "MDSYS.MDPRVT_IDX" WHILE UPGRADING DATABASE TO 18.3
p28730253_190000_Linux-x86-64.zip	Patch 28730253: SUPPORT NEW ERA REIWA FOR JAPANESE IMPERIAL CALENDAR
p29374604_1910000DBRU_Linux-x86-64.zip	Patch 29374604: Golden Gate Integrated Extract not starting 18c/19c Standard Edition
p28852325_190000_Linux-x86-64.zip	DST files - RDBMS - DSTV33 UPDATE - TZDATA2018G - Patch 28852325
p29997937_190000_Linux-x86-64.zip	DST files - RDBMS - DSTV34 UPDATE - TZDATA2019B - Patch 29997937
p31335037_190000_Linux-x86-64.zip	DST files - RDBMS - DSTV35 UPDATE - TZDATA2020A - Patch 31335037
p31335142_190000_Generic.zip	DST files - DSTV35 UPDATE - TZDATA2020A - NEED OJVM FIX - Patch 31335142

To download the database installation files for Oracle Database 18c

1. Go to <https://edelivery.oracle.com/> and sign in.
2. In the box, enter **Oracle Database Enterprise Edition** and choose **Search**.
3. Choose **DLP: Oracle Database 12c Enterprise Edition 18.0.0.0.0 (Oracle Database Enterprise Edition)**.
4. Choose **Continue**.
5. Clear the **Download Queue** check box.
6. Choose **Oracle Database 18.0.0.0.0**.
7. Choose **Linux x86-64** in **Platform/Languages**.
8. Choose **Continue**, and then sign the waiver.

9. Choose **V978967-01.zip**, choose **Download**, and then save the file.

Note

The SHA-256 hash is
C96A4FD768787AF98272008833FE10B172691CF84E42816B138C12D4DE63AB96.

10. Click the links in the following table to download the Oracle patches. All URLs are for updates.oracle.com or support.oracle.com.

File	Description
p6880880_180000_Linux-x86-64.zip	OPatch 12.2.0.1.30 for DB 18.0.0.0.0 (Apr 2022)
p32126855_180000_Linux-x86-64.zip	COMBO OF OJVM RU COMPONENT 18.13.0.0.210119 + DB RU 18.13.0.0.210119
p28730253_180000_Linux-x86-64.zip	SUPPORT NEW ERA REIWA FOR JAPANESE IMPERIAL CALENDAR
p27539475_1813000DBRU_Linux-x86-64.zip	ORA-3816 - MISSING MESSAGE INFORMATION FOR 3816 ERROR
p29213893_180000_Generic.zip	DBMS_STATS FAILING WITH ERROR ORA-01422 WHEN GATHERING STATS FOR USER\$ TABLE
p29374604_1813000DBRU_Linux-x86-64.zip	IE not starting against 18c Oracle RDBMS Standard Edition
p29782284_180000_Generic.zip	ORA-06508: "MDSYS.MDPRVT_IDX" WHILE UPGRADING DATABASE TO 18.3
p28125601_180000_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV32 UPDATE - TZDATA2018E
p28852325_180000_Linux-x86-64.zip	RDBMS - DSTV33 UPDATE - TZDATA2018G
p29997937_180000_Linux-x86-64.zip	RDBMS - DSTV34 UPDATE - TZDATA2019B
p31335037_180000_Linux-x86-64.zip	RDBMS - DSTV35 UPDATE - TZDATA2020A
p31335142_180000_Generic.zip	DSTV35 UPDATE - TZDATA2020A - NEED OJVM FIX

To download the database installation files for Oracle Database 12c Release 2 (12.2)

1. Go to <https://edelivery.oracle.com/> and sign in.
2. In the box, enter **Oracle Database Enterprise Edition** and choose **Search**.
3. Choose **DLP: Oracle Database 12c Enterprise Edition 12.2.0.1.0 (Oracle Database Enterprise Edition)**.
4. Choose **Continue**.
5. Clear the **Download Queue** check box.
6. Choose **Oracle Database 12.2.0.1.0**.
7. Choose **Linux x86-64** in **Platform/Languages**.
8. Choose **Continue**, and then sign the waiver.
9. Choose **V839960-01.zip**, choose **Download**, and then save the file.

Note

The SHA-256 hash is
96ED97D21F15C1AC0CCE3749DA6C3DAC7059BB60672D76B008103FC754D22DDE.

10. Click the links in the following table to download the Oracle patches. All URLs are for updates.oracle.com or support.oracle.com.

File	Description
p6880880_122010_Linux-x86-64.zip	OPatch 12.2.0.1.30 for DB 12.2.0.1.0 (Apr 2022)
p33261817_122010_Linux-x86-64.zip	DATABASE OCT 2021 RELEASE UPDATE 12.2.0.1.211019
p33192662_122010_Linux-x86-64.zip	OJVM RELEASE UPDATE 12.2.0.1.211019
p29213893_122010_Generic.zip	DBMS_STATS FAILING WITH ERROR ORA-01422 WHEN GATHERING STATS FOR USER\$ TABLE
p28730253_122010_Linux-x86-64.zip	SUPPORT NEW ERA REIWA FOR JAPANESE IMPERIAL CALENDAR
p26352615_12201211019DBOCT2021RU_Lin x86-64.zip	SRILLOVER AUDIT FILES CANNOT BE FOUND ORA-46372
p23614158_122010_Linux-x86-64.zip	DSTV27 UPDATE JUNE 2016 - TZDATA2016F
p24701840_122010_Linux-x86-64.zip	RDBMS - DSTV28 UPDATE OCT 2016 - TZDATA2016G
p25173124_122010_Linux-x86-64.zip	RDBMS - DSTV29 UPDATE - TZDATA2016J
p25881255_122010_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV30 UPDATE - TZDATA2017B
p27015449_122010_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV31 UPDATE - TZDATA2017C
p28125601_122010_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV32 UPDATE - TZDATA2018E
p28852325_122010_Linux-x86-64.zip	RDBMS - DSTV33 UPDATE - TZDATA2018G
p29997937_122010_Linux-x86-64.zip	RDBMS - DSTV34 UPDATE - TZDATA2019B
p31335037_122010_Linux-x86-64.zip	RDBMS - DSTV35 UPDATE - TZDATA2020A
p32327201_122010_Linux-x86-64.zip	RDBMS - DSTV36 UPDATE - TZDATA2020E
p32327208_122010_Generic.zip	DSTV36 UPDATE - TZDATA2020E - NEED OJVM FIX

To download the database installation files for Oracle Database 12c Release 1 (12.1)

1. Go to <https://edelivery.oracle.com/> and sign in.
2. In the box, enter **Oracle Database Enterprise Edition** and choose **Search**.
3. Choose **DLP: Oracle Database 12c Enterprise Edition 12.1.0.2.0 (Oracle Database Enterprise Edition)**.
4. Choose **Continue**.
5. Clear the **Download Queue** check box.
6. Choose **Oracle Database 12.1.0.2.0**.
7. Choose **Linux x86-64** in **Platform/Languages**.

8. Choose **Continue**, and then sign the waiver.
9. Choose **V46095-01_1of2.zip** and **V46095-01_2of2.zip**, choose **Download**, and then save the files.

Note

The SHA-256 hash for V46095-01_1of2.zip is

31FDC2AF41687B4E547A3A18F796424D8C1AF36406D2160F65B0AF6A9CD47355.

The SHA-256 hash for V46095-01_2of2.zip is

03DA14F5E875304B28F0F3BB02AF0EC33227885B99C9865DF70749D1E220ACCD.

10. Click the links in the following table to download the Oracle patches. All URLs are for updates.oracle.com or support.oracle.com.

File	Description
p6880880_121010_Linux-x86-64.zip	OPatch 12.2.0.1.29 for DB 12.1.0.1.0 (Feb 2022)
p32768233_121020_Linux-x86-64.zip	DATABASE PATCH SET UPDATE 12.1.0.2.210720
p32876425_121020_Linux-x86-64.zip	OJVM PATCH SET UPDATE 12.1.0.2.210720
p18759211_121020_Linux-x86-64.zip	DST 22: HALF YEARLY DST PATCHES, JUN 2014
p19396455_121020_Linux-x86-64.zip	DST-23: DST UPDATE SEPTEMBER 2014 - TZDATA2014F
p20875898_121020_Linux-x86-64.zip	DST-24: DST UPDATE APRIL 2015 - TZDATA2015D
p22037014_121020_Linux-x86-64.zip	DST-25: DST UPDATE OCTOBER 2015 - TZDATA2015G
p22873635_121020_Linux-x86-64.zip	DST-26: DST UPDATE APRIL 2016 - TZDATA2016D
p23614158_121020_Linux-x86-64.zip	DSTV27 UPDATE JUNE 2016 - TZDATA2016F
p24701840_121020_Linux-x86-64.zip	RDBMS - DSTV28 UPDATE OCT 2016 - TZDATA2016G
p25881255_121020_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV30 UPDATE - TZDATA2017B
p27015449_121020_Linux-x86-64.zip	RDBMS - PROACTIVE DSTV31 UPDATE - TZDATA2017C
p28125601_121020_Linux-x86-64.zip	DSTv32 for RDBMS (TZDATA2018E)
p28852325_121020_Linux-x86-64.zip	DSTv33 for RDBMS (TZDATA2018G)
p29997937_121020_Linux-x86-64.zip	DSTv34 for RDBMS (TZDATA2019G)
p31335037_121020_Linux-x86-64.zip	RDBMS - DSTV35 UPDATE - TZDATA2020A
p32327201_121020_Linux-x86-64.zip	RDBMS - DSTV36 UPDATE - TZDATA2020E
p32327208_121020_Generic.zip	DSTV36 UPDATE - TZDATA2020E - NEED OJVM FIX
p17969866_12102210119_Linux-x86-64.zip	Oracle GoldenGate – 46719 ENH REPLICATION SUPPORT FOR INSERTS / FULL UPDATES WITH LARGE VALUES

File	Description
p20394750_12102210119_Linux-x86-64.zip	Oracle GoldenGate – APPLY CDR RESOLUTION FAILING FOR LOBS, XML, LONG, AND OBJECTS
p24835919_121020_Linux-x86-64.zip	Oracle GoldenGate – IR EXECUTING DEPENDENT TRANSACTIONS OUT OF ORDER WITH PARALLELISM GREATER THAN
p23262847_12102201020_Linux-x86-64.zip	Oracle GoldenGate - MALFORMED REDO CAUSED OGG REPLICATION ABEND
p21171382_12102201020_Generic.zip	ADD CONTROL FOR AUTOMATIC CREATION OF STATS EXTENSIONS
p21091901_12102210720_Linux-x86-64.zip	ONLINE MOVE OF HASH OR REF PARTITION CAN LEAVE LOCAL INDEXES INCONSISTENT
p33013352_12102210720_Linux-x86-64.zip	JSON Bundle Patch
p25031502_12102210720_Linux-x86-64.zip	MV QUERY REWRITE WORKLOAD HIT ORA 600 [KGL-HEAP-SIZE-EXCEEDED]
p23711335_12102191015_Generic.zip	CDB_UPG PDCDB CDB UPGRADE AS WHOLE TAKES 1 MORE HOUR THAN PREVIOUS LABELS IN MAY
p19504946_121020_Linux-x86-64.zip	FLASH CACHE DOESN'T WORK IN OEL7

Uploading your installation files to Amazon S3

Upload your Oracle installation and patch files to Amazon S3 using the AWS CLI. The S3 bucket that contains your installation files must be in the same AWS Region as your CEV.

Choose either of the following options:

- Use `aws s3 cp` to upload a single .zip file.
Upload each installation .zip file separately. Don't combine the .zip files into a single .zip file.
- Use `aws s3 sync` to upload a directory.

List your installation files using either the AWS Management Console or the AWS CLI.

Examples in this section use the following placeholders:

- ***install-or-patch-file.zip*** – Oracle installation media file. For example, p32126828_190000_Linux-x86-64.zip is a patch.
- ***my-custom-installation-files*** – Your Amazon S3 bucket designated for your uploaded installation files.
- ***123456789012/cev1*** – An optional prefix in your Amazon S3 bucket.
- ***source-bucket*** – An Amazon S3 bucket where you can optionally stage files.

The following example uploads ***install-or-patch-file.zip*** to the ***123456789012/cev1*** folder in the RDS Custom Amazon S3 bucket. Run a separate `aws s3` command for each .zip that you want to upload.

For Linux, macOS, or Unix:

```
aws s3 cp install-or-patch-file.zip \  
s3://my-custom-installation-files/123456789012/cev1/
```

For Windows:

```
aws s3 cp install-or-patch-file.zip ^  
s3://my-custom-installation-files/123456789012/cev1/
```

Verify that your S3 bucket is in the AWS Region where you plan to run the `create-custom-db-engine-version` command.

```
aws s3api get-bucket-location --bucket my-custom-installation-files
```

List the files in your RDS Custom Amazon S3 bucket as follows.

```
aws s3 ls \  
s3://my-custom-installation-files/123456789012/cev1/
```

The following example uploads the files in your local `cev1` folder to the `123456789012/cev1` folder in your Amazon S3 bucket.

For Linux, macOS, or Unix:

```
aws s3 sync cev1 \  
s3://my-custom-installation-files/123456789012/cev1/
```

For Windows:

```
aws s3 sync cev1 ^  
s3://my-custom-installation-files/123456789012/cev1/
```

The following example uploads all files in `source-bucket` to the `123456789012/cev1` folder in your Amazon S3 bucket.

For Linux, macOS, or Unix:

```
aws s3 sync s3://source-bucket/ \  
s3://my-custom-installation-files/123456789012/cev1/
```

For Windows:

```
aws s3 sync s3://source-bucket/ ^  
s3://my-custom-installation-files/123456789012/cev1/
```

Sharing your installation media in S3 across AWS accounts

For the purposes of this section, the Amazon S3 bucket that contains your uploaded Oracle installation files is your *media bucket*. Your organization might use multiple AWS accounts in an AWS Region. If so, you might want to use one AWS account to populate your media bucket and a different AWS account to create CEVs. If you don't intend to share your media bucket, skip to the next section.

This section assumes the following:

- You can access the account that created your media bucket and a different account in which you intend to create CEVs.

- You intend to create CEVs in only one AWS Region. If you intend to use multiple Regions, create a media bucket in each Region.
- You're using the CLI. If you're using the Amazon S3 console, adapt the following steps.

To configure your media bucket for sharing across AWS accounts

1. Log in to the AWS account that contains the S3 bucket into which you uploaded your installation media.
2. Start with either a blank JSON policy template or an existing policy that you can adapt.

The following command retrieves an existing policy and saves it as *my-policy.json*. In this example, the S3 bucket containing your installation files is named *oracle-media-bucket*.

```
aws s3api get-bucket-policy \
--bucket oracle-media-bucket \
--query Policy \
--output text > my-policy.json
```

3. Edit the media bucket permissions as follows:

- In the Resource element of your template, specify the S3 bucket into which you uploaded your Oracle Database installation files.
- In the Principal element, specify the ARNs for all AWS accounts that you intend to use to create CEVs. You can add the root, a user, or a role to the S3 bucket allow list. For more information, see [IAM identifiers](#) in the *AWS Identity and Access Management User Guide*.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "GrantAccountsAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-1:root",
                    "arn:aws:iam::account-2:user/user-name-with-path",
                    "arn:aws:iam::account-3:role/role-name-with-path",
                    ...
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3>ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::oracle-media-bucket",
                "arn:aws:s3:::oracle-media-bucket/*"
            ]
        }
    ]
}
```

4. Attach the policy to your media bucket.

In the following example, *oracle-media-bucket* is the name of the S3 bucket that contains your installation files, and *my-policy.json* is the name of your JSON file.

```
aws s3api put-bucket-policy \
--bucket oracle-media-bucket \
--policy file://my-policy.json
```

5. Log in to an AWS account in which you intend to create CEVs.
6. Verify that this account can access the media bucket in the AWS account that created it.

```
aws s3 ls --query "Buckets[] .Name"
```

For more information, see [aws s3 ls](#) in the *AWS CLI Command Reference*.

7. Create a CEV by following the steps in [Creating a CEV \(p. 798\)](#).

Preparing the CEV manifest

A *CEV manifest* is a JSON document that includes the following:

- (Required) The list of installation .zip files that you uploaded to Amazon S3. RDS Custom applies the patches in the order in which they're listed in the manifest.
- (Optional) Installation parameters that set nondefault values for the Oracle base, Oracle home, and the ID and name of the UNIX/Linux user and group. Be aware that you can't modify the installation parameters for an existing CEV or an existing DB instance. You also can't upgrade from one CEV to another CEV when the installation parameters have different settings.

For sample CEV manifests, see [CEV manifest examples \(p. 795\)](#).

Topics

- [JSON fields in the CEV manifest \(p. 789\)](#)
- [Creating the CEV manifest \(p. 795\)](#)
- [CEV manifest examples \(p. 795\)](#)

JSON fields in the CEV manifest

The following table describes the JSON fields in the manifest.

JSON fields in the CEV manifest

JSON field	Description
MediaImportTemplateVersion	Version of the CEV manifest. The date is in the format YYYY-MM-DD.
databaseInstallationFileName	Ordered list of installation files for the database.
opatchFileNames	Ordered list of OPatch installers used for the Oracle DB engine. Only one value is valid. Values for opatchFileNames must start with p6880880_.
psuRuPatchFileNames	The PSU and RU patches for this database. Important If you include psuRuPatchFileNames, opatchFileNames is required. Values for opatchFileNames must start with p6880880_. The PSU and RU patches for this database.
OtherPatchFileNames	The patches that aren't in the list of PSU and RU patches. RDS Custom applies these patches after applying the PSU and RU patches.

JSON field	Description
	<p>Important If you include OtherPatchFileNames, opatchFileNames is required. Values for opatchFileNames must start with p6880880_.</p>

JSON field	Description
installationParameters	<p>Nondefault settings for the Oracle base, Oracle home, and the ID and name of the UNIX/Linux user and group. You can set the following parameters:</p> <p>oracleBase</p> <p>The directory under which your Oracle binaries are installed. It is the mount point of the binary volume that stores your files. The Oracle base directory can include multiple Oracle homes. For example, if /home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1 is one of your Oracle home directories, then /home/oracle is the Oracle base directory. A user-specified Oracle base directory is not a symbolic link.</p> <p>If you don't specify the Oracle base, the default directory is /rdsdbbin.</p> <p>oracleHome</p> <p>The directory in which your Oracle database binaries are installed. For example, if you specify /home/oracle/ as your Oracle base, then you might specify /home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1/ as your Oracle home. A user-specified Oracle home directory is not a symbolic link. The Oracle home value is referenced by the \$ORACLE_HOME environment variable.</p> <p>If you don't specify the Oracle home, the default naming format is /rdsdbbin/oracle.<i>major-engine-version</i>.custom.r1.<i>engine-edition</i>.1.</p> <p>unixUsername</p> <p>The name of the UNIX user that owns the Oracle software. RDS Custom assumes this user when running local database commands. If you specify both unixUid and unixUsername, RDS Custom creates the user if it doesn't exist, and then assigns the UID to the user if it's not the same as the initial UID.</p> <p>The default user name is rdsdb.</p> <p>unixUserId</p> <p>The ID (UID) of the UNIX user that owns the Oracle software. If you specify both unixUid and unixUsername, RDS Custom creates the user if it doesn't exist, and then assigns the UID to the user if it's not the same as the initial UID.</p> <p>The default UID is 61001. This is the UID of the user rdsdb.</p> <p>unixGroupName</p> <p>The name of the UNIX group. The UNIX user that owns the Oracle software belongs to this group.</p> <p>The default group name is rdsdb.</p> <p>unixGroupId</p> <p>The ID of the UNIX group to which the UNIX user belongs.</p> <p>The default group ID is 1000. This is the ID of the group rdsdb.</p>

Each Oracle Database release has a different list of supported installation files. When you create your CEV manifest, make sure to specify only files that are supported by RDS Custom for Oracle. Otherwise, CEV creation fails with an error.

The following table shows valid values for Oracle Database 12c Release 1 (12.1).

Valid values for Oracle Database 12c Release 1 (12.1)

JSON field	Valid values for 12.1
MediaImportTemplateVersion	2020-08-14
databaseInstallationFileNames	V46095-01_1of2.zip V46095-01_2of2.zip
opatchFileNames	p6880880_121010_Linux-x86-64.zip
psuRuPatchFileNames	p32768233_121020_Linux-x86-64.zip
OtherPatchFileNames	p32876425_121020_Linux-x86-64.zip p18759211_121020_Linux-x86-64.zip p19396455_121020_Linux-x86-64.zip p20875898_121020_Linux-x86-64.zip p22037014_121020_Linux-x86-64.zip p22873635_121020_Linux-x86-64.zip p23614158_121020_Linux-x86-64.zip p24701840_121020_Linux-x86-64.zip p25881255_121020_Linux-x86-64.zip p27015449_121020_Linux-x86-64.zip p28125601_121020_Linux-x86-64.zip p28852325_121020_Linux-x86-64.zip p29997937_121020_Linux-x86-64.zip p31335037_121020_Linux-x86-64.zip p32327201_121020_Linux-x86-64.zip p32327208_121020_Generic.zip p17969866_12102210119_Linux-x86-64.zip p20394750_12102210119_Linux-x86-64.zip p24835919_121020_Linux-x86-64.zip p23262847_12102201020_Linux-x86-64.zip p21171382_12102201020_Generic.zip

JSON field	Valid values for 12.1
	p21091901_12102210720_Linux-x86-64.zip p33013352_12102210720_Linux-x86-64.zip p25031502_12102210720_Linux-x86-64.zip p23711335_12102191015_Generic.zip p19504946_121020_Linux-x86-64.zip

The following table shows valid values for Oracle Database 12c Release 2 (12.2).

Valid values for Oracle Database 12c Release 2 (12.2)

JSON field	Valid values for Oracle Database 12c Release 2 (12.2)
MediaImportTemplateVersion	2020-08-14
databaseInstallationFileNames	SV839960-01.zip
opatchFileNames	p6880880_122010_Linux-x86-64.zip
psuRuPatchFileNames	p33261817_122010_Linux-x86-64.zip
OtherPatchFileNames	p33192662_122010_Linux-x86-64.zip p29213893_122010_Generic.zip p28730253_122010_Linux-x86-64.zip p26352615_12201211019DBOCT2021RU_Linux-x86-64.zip p23614158_122010_Linux-x86-64.zip p24701840_122010_Linux-x86-64.zip p25173124_122010_Linux-x86-64.zip p25881255_122010_Linux-x86-64.zip p27015449_122010_Linux-x86-64.zip p28125601_122010_Linux-x86-64.zip p28852325_122010_Linux-x86-64.zip p29997937_122010_Linux-x86-64.zip p31335037_122010_Linux-x86-64.zip p32327201_122010_Linux-x86-64.zip p32327208_122010_Generic.zip

The following table shows valid values for Oracle Database 18c.

Valid values for Oracle Database 18c

JSON field	Valid values for 18c
MediaImportTemplateVersion	2020-08-14
databaseInstallationFileName	v978967-01.zip
opatchFileNames	p6880880_180000_Linux-x86-64.zip
psuRuPatchFileNames	p32126855_180000_Linux-x86-64.zip
OtherPatchFileNames	p28730253_180000_Linux-x86-64.zip p27539475_1813000DBRU_Linux-x86-64.zip p29213893_180000_Generic.zip p29374604_1813000DBRU_Linux-x86-64.zip p29782284_180000_Generic.zip p28125601_180000_Linux-x86-64.zip p28852325_180000_Linux-x86-64.zip p29997937_180000_Linux-x86-64.zip p31335037_180000_Linux-x86-64.zip p31335142_180000_Generic.zip

The following table shows valid values for Oracle Database 19c.

Valid values for Oracle Database 19c

JSON field	Valid values for 19c
MediaImportTemplateVersion	2020-08-14
databaseInstallationFileName	v982063-01.zip
opatchFileNames	p6880880_190000_Linux-x86-64.zip
psuRuPatchFileNames	p32126828_190000_Linux-x86-64.zip
OtherPatchFileNames	p29213893_1910000DBRU_Generic.zip p29782284_1910000DBRU_Generic.zip p28730253_190000_Linux-x86-64.zip p29374604_1910000DBRU_Linux-x86-64.zip p28852325_190000_Linux-x86-64.zip p29997937_190000_Linux-x86-64.zip p31335037_190000_Linux-x86-64.zip p31335142_190000_Generic.zip

Creating the CEV manifest

To create a CEV manifest

1. List all installation files that you plan to apply, in the order that you want to apply them.
2. Correlate the installation files with the JSON fields described in [JSON fields in the CEV manifest \(p. 789\)](#).
3. Do either of the following:
 - Create the CEV manifest as a JSON text file.
 - Edit the CEV manifest template when you create the CEV in the console. For more information, see [Creating a CEV \(p. 798\)](#).

CEV manifest examples

The following examples show CEV manifest files for different Oracle Database releases. If you include a JSON field in your manifest, make sure that it isn't empty. For example, the following CEV manifest isn't valid because otherPatchFileNames is empty.

```
{  
    "mediaImportTemplateVersion": "2020-08-14",  
    "databaseInstallationFileNames": [  
        "V982063-01.zip"  
    ],  
    "opatchFileNames": [  
        "p6880880_190000_Linux-x86-64.zip"  
    ],  
    "psuRuPatchFileNames": [  
        "p32126828_190000_Linux-x86-64.zip"  
    ],  
    "otherPatchFileNames": [  
    ]  
}
```

Topics

- [Sample CEV manifest for Oracle Database 12c Release 1 \(12.1\) \(p. 795\)](#)
- [Sample CEV manifest for Oracle Database 12c Release 2 \(12.2\) \(p. 796\)](#)
- [Sample CEV manifest for Oracle Database 18c \(p. 797\)](#)
- [Sample CEV manifest for Oracle Database 19c \(p. 797\)](#)

Example Sample CEV manifest for Oracle Database 12c Release 1 (12.1)

In the following example for the July 2021 PSU for Oracle Database 12c Release 1 (12.1), RDS Custom applies the patches in the order specified. Thus, RDS Custom applies p32768233, then p32876425, then p18759211, and so on. The example sets new values for the UNIX user and group, and the Oracle home and Oracle base.

```
{  
    "mediaImportTemplateVersion": "2020-08-14",  
    "databaseInstallationFileNames": [  
        "V46095-01_1of2.zip",  
        "V46095-01_2of2.zip"  
    ],  
    "opatchFileNames": [  
        "p6880880_121010_Linux-x86-64.zip"  
    ],  
    "psuRuPatchFileNames": [  
    ]  
}
```

```

"psuRuPatchFileNames": [
    "p32768233_121020_Linux-x86-64.zip"
],
"otherPatchFileNames": [
    "p32876425_121020_Linux-x86-64.zip",
    "p18759211_121020_Linux-x86-64.zip",
    "p19396455_121020_Linux-x86-64.zip",
    "p20875898_121020_Linux-x86-64.zip",
    "p22037014_121020_Linux-x86-64.zip",
    "p22873635_121020_Linux-x86-64.zip",
    "p23614158_121020_Linux-x86-64.zip",
    "p24701840_121020_Linux-x86-64.zip",
    "p25881255_121020_Linux-x86-64.zip",
    "p27015449_121020_Linux-x86-64.zip",
    "p28125601_121020_Linux-x86-64.zip",
    "p28852325_121020_Linux-x86-64.zip",
    "p29997937_121020_Linux-x86-64.zip",
    "p31335037_121020_Linux-x86-64.zip",
    "p32327201_121020_Linux-x86-64.zip",
    "p32327208_121020_Generic.zip",
    "p17969866_12102210119_Linux-x86-64.zip",
    "p20394750_12102210119_Linux-x86-64.zip",
    "p24835919_121020_Linux-x86-64.zip",
    "p23262847_12102201020_Linux-x86-64.zip",
    "p21171382_12102201020_Generic.zip",
    "p21091901_12102210720_Linux-x86-64.zip",
    "p33013352_12102210720_Linux-x86-64.zip",
    "p25031502_12102210720_Linux-x86-64.zip",
    "p23711335_12102191015_Generic.zip",
    "p19504946_121020_Linux-x86-64.zip"
],
"installationParameters": {
    "unixGroupName": "dba",
    "unixUname": "oracle",
    "oracleHome": "/home/oracle/oracle.12.1.0.2",
    "oracleBase": "/home/oracle"
}
}

```

Example Sample CEV manifest for Oracle Database 12c Release 2 (12.2)

In following example for the October 2021 PSU for Oracle Database 12c Release 2 (12.2), RDS Custom applies p33261817, then p33192662, then p29213893, and so on. The example sets new values for the UNIX user and group, and the Oracle home and Oracle base.

```

{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V839960-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_122010_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p33261817_122010_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
        "p33192662_122010_Linux-x86-64.zip",
        "p29213893_122010_Generic.zip",
        "p28730253_122010_Linux-x86-64.zip",
        "p26352615_12201211019DBOCT2021RU_Linux-x86-64.zip",
        "p23614158_122010_Linux-x86-64.zip",
        "p24701840_122010_Linux-x86-64.zip",
        "p25173124_122010_Linux-x86-64.zip",

```

```

    "p25881255_122010_Linux-x86-64.zip",
    "p27015449_122010_Linux-x86-64.zip",
    "p28125601_122010_Linux-x86-64.zip",
    "p28852325_122010_Linux-x86-64.zip",
    "p29997937_122010_Linux-x86-64.zip",
    "p31335037_122010_Linux-x86-64.zip",
    "p32327201_122010_Linux-x86-64.zip",
    "p32327208_122010_Generic.zip"
],
"installationParameters": {
    "unixGroupName": "dba",
    "unixUname": "oracle",
    "oracleHome": "/home/oracle/oracle.12.2.0.1",
    "oracleBase": "/home/oracle"
}
}

```

Example Sample CEV manifest for Oracle Database 18c

In following example for the October 2021 PSU for Oracle Database 18c, RDS Custom applies p32126855, then p28730253, then p27539475, and so on. The example sets new values for the UNIX user and group, and the Oracle home and Oracle base.

```

{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V978967-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_180000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p32126855_180000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
        "p28730253_180000_Linux-x86-64.zip",
        "p27539475_1813000DBRU_Linux-x86-64.zip",
        "p29213893_180000_Generic.zip",
        "p29374604_1813000DBRU_Linux-x86-64.zip",
        "p29782284_180000_Generic.zip",
        "p28125601_180000_Linux-x86-64.zip",
        "p28852325_180000_Linux-x86-64.zip",
        "p29997937_180000_Linux-x86-64.zip",
        "p31335037_180000_Linux-x86-64.zip",
        "p31335142_180000_Generic.zip"
    ],
    "installationParameters": {
        "unixGroupName": "dba",
        "unixUname": "oracle",
        "oracleHome": "/home/oracle/18.0.0.0.ru-2020-10.rur-2020-10.r1",
        "oracleBase": "/home/oracle/"
    }
}

```

Example Sample CEV manifest for Oracle Database 19c

In the following example for Oracle Database 19c, RDS Custom applies p32126828, then p29213893, then p29782284, and so on. The example sets new values for the UNIX user and group, and the Oracle home and Oracle base.

```
{
    "mediaImportTemplateVersion": "2020-08-14",
```

```
"databaseInstallationFileNames": [
    "V982063-01.zip"
],
"opatchFileNames": [
    "p6880880_190000_Linux-x86-64.zip"
],
"psuRuPatchFileNames": [
    "p32126828_190000_Linux-x86-64.zip"
],
"otherPatchFileNames": [
    "p29213893_1910000DBRU_Generic.zip",
    "p29782284_1910000DBRU_Generic.zip",
    "p28730253_190000_Linux-x86-64.zip",
    "p29374604_1910000DBRU_Linux-x86-64.zip",
    "p28852325_190000_Linux-x86-64.zip",
    "p29997937_190000_Linux-x86-64.zip",
    "p31335037_190000_Linux-x86-64.zip",
    "p31335142_190000_Generic.zip"
],
"installationParameters": {
    "unixGroupName": "dba",
    "unixUname": "oracle",
    "oracleHome": "/home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1",
    "oracleBase": "/home/oracle"
}
}
```

Validating the CEV manifest

Optionally, verify that manifest is a valid JSON file by running the `json.tool` Python script.

For example, if you change into the directory containing a CEV manifest named `manifest.json`, run the following command.

```
python -m json.tool < manifest.json
```

Adding necessary IAM permissions

Make sure that the IAM principal that creates the CEV has the necessary policies described in [Grant required permissions to your IAM user \(p. 778\)](#).

Creating a CEV

You can create a CEV using the AWS Management Console or the AWS CLI. Typically, creating a CEV takes about two hours.

You can then use the CEV to create an RDS Custom instance. Make sure that the Amazon S3 bucket containing your installation files is in the same AWS Region as your CEV. Otherwise, the process to create a CEV fails.

For more information, see [Creating an RDS Custom for Oracle DB instance \(p. 808\)](#).

Console

To create a CEV

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Custom engine versions**.

The **Custom engine versions** page shows all CEVs that currently exist. If you haven't created any CEVs, the page is empty.

3. Choose **Create custom engine version**.
4. For **Engine type**, choose **Oracle**.
5. For **Edition**, choose **Oracle Enterprise Edition**. **Oracle Enterprise Edition (Oracle RAC option)** isn't supported.
6. For **Architecture settings**, choose **Multitenant architecture** to create a Multitenant CEV, which uses the engine `custom-oracle-ee-cdb`. You can create an RDS Custom for Oracle CDB with a Multitenant CEV only. If you don't choose this option, your CEV is a non-CDB, which uses the engine `custom-oracle-ee`.
7. For **Major version**, choose the major engine version.
8. In **Version details**, enter a valid name in **Custom engine version name**.

The name format is `major-engine-version.customized_string`. You can use 1–50 alphanumeric characters, underscores, dashes, and periods. For example, you might enter the name **19.cdb_cev1**.

Optionally, enter a description for your CEV.

9. For **S3 location of manifest files**, enter the location of the Amazon S3 bucket that you specified in [Uploading your installation files to Amazon S3 \(p. 786\)](#). For example, enter `s3://my-custom-installation-files/806242271698/cev1/`.
10. In the **RDS Custom encryption** section, select **Enter a key ARN** to list the available AWS KMS keys.

Then select your KMS key from the list. An AWS KMS key is required for RDS Custom. For more information, see [Make sure that you have a symmetric encryption AWS KMS key \(p. 768\)](#).

11. Choose **Create custom engine version**.

If the CEV manifest has an invalid form, the console displays **Error validating the CEV manifest**. Fix the problems, and try again.

The **Custom engine versions** page appears. Your CEV is shown with the status **Creating**. The process to create the CEV takes approximately two hours.

AWS CLI

To create a CEV by using the AWS CLI, run the `create-custom-db-engine-version` command.

The following options are required:

- `--engine engine-type`, where `engine-type` is either `custom-oracle-ee-cdb` for a CDB or `custom-oracle-ee` for a non-CDB. You can create CDBs only from a CEV created with `custom-oracle-ee-cdb`. You can create non-CDBs only from a CEV created with `custom-oracle-ee`.
- `--engine-version major-engine-version.customized_string`
- `--kms-key-id`
- `--manifest manifest_string` or `--manifest file:file_name`

Newline characters aren't permitted in `manifest_string`. Make sure to escape double quotes ("") in the JSON code by prefixing them with a backslash (\).

The following example shows the `manifest_string` for 19c from [Preparing the CEV manifest \(p. 789\)](#). The example sets new values for the Oracle base, Oracle home, and the ID and name of the UNIX/Linux user and group. If you copy this string, remove all newline characters before pasting it into your command.

```
"{\"mediaImportTemplateVersion\": \"2020-08-14\",
\"databaseInstallationFileNames\": [\"V982063-01.zip\"],
\"opatchFileNames\": [\"p6880880_190000_Linux-x86-64.zip\"],
\"psuRuPatchFileNames\": [\"p32126828_190000_Linux-x86-64.zip\"],
\"otherPatchFileNames\": [\"p29213893_1910000DBRU_Generic.zip\",
\"p29782284_1910000DBRU_Generic.zip\", \"p28730253_190000_Linux-x86-64.zip\",
\"p29374604_1910000DBRU_Linux-x86-64.zip\", \"p28852325_190000_Linux-
x86-64.zip\", \"p29997937_190000_Linux-x86-64.zip\", \"p31335037_190000_Linux-
x86-64.zip\", \"p31335142_190000_Generic.zip\"]}\"installationParameters\":
{ \"unixGroupName\":\"dba\", \\"unixUname\":\"oracle\", \\"oracleHome\":\"/\"/
home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1\", \\"oracleBase
\":\"/home/oracle/\\"}}}"
• --database-installation-files-s3-bucket-name s3-bucket-name, where s3-
bucket-name is the bucket name that you specified in Uploading your installation files to Amazon S3 \(p. 786\). The AWS Region in which you run create-custom-db-engine-version must be the same Region as your Amazon S3 bucket.
```

You can also specify the following options:

- `--description my-cev-description`
- `database-installation-files-s3-prefix prefix`, where *prefix* is the folder name that you specified in [Uploading your installation files to Amazon S3 \(p. 786\)](#).

The following example creates a Multitenant CEV named `19.cdb_cev1`. Make sure that the name of your CEV starts with the major engine version number.

Example

For Linux, macOS, or Unix:

```
aws rds create-custom-db-engine-version \
--engine custom-oracle-ee-cdb \
--engine-version 19.cdb_cev1 \
--database-installation-files-s3-bucket-name my-custom-installation-files \
--database-installation-files-s3-prefix 123456789012/cev1 \
--kms-key-id my-kms-key \
--description "some text" \
--manifest manifest_string
```

For Windows:

```
aws rds create-custom-db-engine-version ^
--engine custom-oracle-ee-cdb ^
--engine-version 19.cdb_cev1 ^
--database-installation-files-s3-bucket-name s3://my-custom-installation-files ^
--database-installation-files-s3-prefix 123456789012/cev1 ^
--kms-key-id my-kms-key ^
--description "some text" ^
--manifest manifest_string
```

Example

Get details about your CEV by using the `describe-db-engine-versions` command.

```
aws rds describe-db-engine-versions \
```

```
--engine custom-oracle-ee-cdb \
--include-all
```

The following partial sample output shows the engine, parameter groups, manifest, and other information.

```
"DBEngineVersions": [
  {
    "Engine": "custom-oracle-ee",
    "MajorEngineVersion": "19",
    "EngineVersion": "19.cev.2021-01.08",
    "DatabaseInstallationFilesS3BucketName": "us-east-1-123456789012-cev-custom-
installation-files",
    "DatabaseInstallationFilesS3Prefix": "123456789012/cev1",
    "CustomDBEngineVersionManifest": "{\n\"mediaImportTemplateVersion\":
\"2020-08-14\",\\n\"databaseInstallationFileNames\": [\\n\"V982063-01.zip\\n],\\n
\"installationParameters\": {\\n\"oracleBase\": \"/tmp\",\\n\"oracleHome\": \"/tmp/Oracle\\n},
\\n\"patchFileNames\": [\\n\"p6880880_190000_Linux-x86-64.zip\\n],\\n\"psuRuPatchFileNames
\": [\\n\"p32126828_190000_Linux-x86-64.zip\\n],\\n\"otherPatchFileNames\": [\\n
\"p29213893_1910000DBRU_Generic.zip\",\\n\"p29782284_1910000DBRU_Generic.zip\",\\n
\"p28730253_190000_Linux-x86-64.zip\",\\n\"p29374604_1910000DBRU_Linux-x86-64.zip\",
\\n\"p28852325_190000_Linux-x86-64.zip\",\\n\"p29997937_190000_Linux-x86-64.zip\",\\n
\"p31335037_190000_Linux-x86-64.zip\",\\n\"p31335142_190000_Generic.zip\\n]\\n}\\n",
    "DBParameterGroupFamily": "custom-oracle-ee-19",
    "DBEngineDescription": "Oracle Database server EE for RDS Custom",
    "DBEngineVersionArn": "arn:aws:rds:us-west-2:123456789012:cev:custom-oracle-
ee/19.my_cev1/0a123b45-6c78-901d-23e4-5678f901fg23",
    "DBEngineVersionDescription": "test",
    "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/ab1c2de3-f4g5-6789-h012-
h3ijk4567189",
    "CreateTime": "2022-11-18T09:17:07.693000+00:00",
    "ValidUpgradeTarget": [
      {
        "Engine": "custom-oracle-ee",
        "EngineVersion": "19.cev.2021-01.09",
        "Description": "test",
        "AutoUpgrade": false,
        "IsMajorVersionUpgrade": false
      }
    ]
}
```

Failure to create a CEV

If the process to create a CEV fails, RDS Custom issues RDS-EVENT-0198 with the message **Creation failed for custom engine version *major-engine-version.cev_name***, and includes details about the failure. For example, the event prints missing files.

You can't modify a failed CEV. You can only delete it, then try again to create a CEV after fixing the causes of the failure. For information about troubleshooting the reasons for CEV creation failure, see [Troubleshooting custom engine version creation for RDS Custom for Oracle \(p. 890\)](#).

Modifying CEV status

You can modify a CEV using the AWS Management Console or the AWS CLI. You can modify the CEV description or its availability status. Your CEV has one of the following status values:

- **available** – You can use this CEV to create a new RDS Custom DB instance or upgrade a DB instance. This is the default status for a newly created CEV.
- **inactive** – You can't create or upgrade an RDS Custom instance with this CEV. You can't restore a DB snapshot to create a new RDS Custom DB instance with this CEV.

You can change the CEV from any supported status to any other supported status. You might change status to prevent the accidental use of a CEV or make a discontinued CEV eligible for use again. For example, you might change the status of your CEV from available to inactive, and from inactive back to available.

Console

To modify a CEV

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Custom engine versions**.
3. Choose a CEV whose description or status you want to modify.
4. For **Actions**, choose **Modify**.
5. Make any of the following changes:
 - For **CEV status settings**, choose a new availability status.
 - For **Version description**, enter a new description.
6. Choose **Modify CEV**.

If the CEV is in use, the console displays **You can't modify the CEV status**. Fix the problems, and try again.

The **Custom engine versions** page appears.

AWS CLI

To modify a CEV by using the AWS CLI, run the `modify-custom-db-engine-version` command. You can find CEVs to modify by running the `describe-db-engine-versions` command.

The following options are required:

- `--engine custom-oracle-ee`
- `--engine-version cev`, where *cev* is the name of the custom engine version that you want to modify
- `--status status`, where *status* is the availability status that you want to assign to the CEV

The following example changes a CEV named `19.my_cev1` from its current status to `inactive`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-custom-db-engine-version \
    --engine custom-oracle-ee \
    --engine-version 19.my_cev1 \
    --status inactive
```

For Windows:

```
aws rds modify-custom-db-engine-version ^
    --engine custom-oracle-ee ^
    --engine-version 19.my_cev1 ^
    --status inactive
```

Viewing CEV details

You can view details about your CEV manifest and the command used to create your CEV by using the AWS Management Console or the AWS CLI.

Console

To view CEV details

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Custom engine versions**.

The **Custom engine versions** page shows all CEVs that currently exist. If you haven't created any CEVs, the page is empty.

3. Choose the name of the CEV that you want to view.
4. Choose **Configuration** to view the installation parameters specified in your manifest.

Configuration	Databases	Snapshots	Manifest
Configuration			
<p>Edition Oracle Enterprise Edition</p> <p>Major Version 19</p> <p>Installation files location s3://.../V982063-01.zip</p>	<p>Amazon Resource Name (ARN) arn:aws:rds:us-west-2: .../rdsdbbin/oracle.19.custom.r1.EE.1</p> <p>KMS key ID .../p30528704_197000DBRU_Linux-x86-64.zip</p>	<p>DB installation parameters</p> <p>Oracle Base Directory /rdsdbbin</p> <p>Oracle Home Directory /rdsdbbin/oracle.19.custom.r1.EE.1</p> <p>Oracle User Name rdsdb</p> <p>Oracle UID 61001</p> <p>Oracle Group Name rdsdb</p> <p>Oracle GID 1000</p>	

5. Choose **Manifest** to view the installation parameters specified in the --manifest option of the create-custom-db-engine-version command. You can copy this text, replace values as needed, and use them in a new command.

Configuration	Databases	Snapshots	Automated Backups	Tags	Manifest
CEV manifest					
<pre>--manifest "{\"databaseInstallationFileNames\": [\"V982063-01.zip\"], \"mediaImportTemplateVersion\": \"2020-08-14\", \"opatchFileNames\":\n[\"p6880880_190000_1220119_Linux-x86-64.zip\"], \"psuRuPatchFileNames\": [\"p30783543_190000_Linux-x86-64.zip\", \"p30528704_197000DBRU_Linux-\nx86-64.zip\", \"p29213893_197000DBRU_Generic.zip\", \"p28730253_190000_Linux-x86-64.zip\"], \"p28852325_190000_Linux-x86-\n64.zip\", \"p29997937_190000_Linux-x86-64.zip\", \"p29997959_190000_Generic.zip\"], \"installationParameters\":\n{\"oracleHome\": \"/rdsdbbin/oracle.19.custom.r1.EE.1\", \"oracleBase\": \"/rdsdbbin\", \"unixUid\": 61001, \"unixUsername\": \"rdsdb\", \"unixGroupId\": 1000, \"unixGroup\nname\": \"rdsdb\"}}"</pre>					

AWS CLI

To view details about a CEV by using the AWS CLI, run the [describe-db-engine-versions](#) command.

The following options are required:

- `--engine custom-oracle-ee`
- `--engine-version major-engine-version.customized_string`

The following example creates a CEV named `19.my_cev1`. Make sure that the name of your CEV starts with the major engine version number.

Example

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine custom-oracle-ee \
--engine-version 19.my_cev1
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine custom-oracle-ee ^
--engine-version 19.my_cev1
```

The following partial sample output shows the engine, parameter groups, manifest, and other information.

```
"DBEngineVersions": [
  {
    "Engine": "custom-oracle-ee",
    "MajorEngineVersion": "19",
    "EngineVersion": "19.my_cev1",
    "DatabaseInstallationFilesS3BucketName": "us-east-1-123456789012-cev-customer-
installation-files",
    "DatabaseInstallationFilesS3Prefix": "123456789012/cev1",
    "CustomDBEngineVersionManifest": "{\n\"mediaImportTemplateVersion\": \"2020-08-14\", \n\"databaseInstallationFileNames\": [\n\"V982063-01.zip\\n\"], \n\"installationParameters\": {\n\"oracleBase\": \"/tmp\", \n\"oracleHome\": \"/tmp/Oracle\\n\"}, \n\"opatchFileNames\": [\n\"p6880880_190000_Linux-x86-64.zip\\n\"], \n\"psuRuPatchFileNames\": [\n\"p32126828_190000_Linux-x86-64.zip\\n\"], \n\"otherPatchFileNames\": [\n\"p29213893_1910000DBRU_Generic.zip\", \n\"p29782284_1910000DBRU_Generic.zip\\n\", \n\"p28730253_190000_Linux-x86-64.zip\\n\", \n\"p29374604_1910000DBRU_Linux-x86-64.zip\\n\", \n\"p28852325_190000_Linux-x86-64.zip\\n\", \n\"p29997937_190000_Linux-x86-64.zip\\n\", \n\"p31335037_190000_Linux-x86-64.zip\\n\", \n\"p31335142_190000_Generic.zip\\n]\\n} \\n",
    "DBParameterGroupFamily": "custom-oracle-ee-19",
    "DBEngineDescription": "Oracle Database server EE for RDS Custom",
    "DBEngineVersionArn": "arn:aws:rds:us-west-2:123456789012:cev:custom-oracle-
ee/19.my_cev1/0a123b45-6c78-901d-23e4-5678f901fg23",
    "DBEngineVersionDescription": "test",
    "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/ab1c2de3-f4g5-6789-h012-
h3ijk4567189",
    "CreateTime": "2022-11-18T09:17:07.693000+00:00",
    "ValidUpgradeTarget": [
      {
        "Engine": "custom-oracle-ee",
        "EngineVersion": "19.cev.2021-01.09",
        "Description": "test",
        "AutoUpgrade": false,
      }
    ]
  }
]
```

```
        "IsMajorVersionUpgrade": false
    }
```

Deleting a CEV

You can delete a CEV using the AWS Management Console or the AWS CLI. Typically, deletion takes a few minutes.

To delete a CEV, it can't be in use by any of the following:

- An RDS Custom DB instance
- A snapshot of an RDS Custom DB instance
- An automated backup of your RDS Custom DB instance

Console

To delete a CEV

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Custom engine versions**.
3. Choose a CEV whose description or status you want to delete.
4. For **Actions**, choose **Delete**.

The **Delete *cev_name*?** dialog box appears.

5. Enter **delete me**, and then choose **Delete**.

In the **Custom engine versions** page, the banner shows that your CEV is being deleted.

AWS CLI

To delete a CEV by using the AWS CLI, run the `delete-custom-db-engine-version` command.

The following options are required:

- `--engine custom-oracle-ee`
- `--engine-version cev`, where *cev* is the name of the custom engine version to be deleted

The following example deletes a CEV named `19.my_cev1`.

Example

For Linux, macOS, or Unix:

```
aws rds delete-custom-db-engine-version \
--engine custom-oracle-ee \
--engine-version 19.my_cev1
```

For Windows:

```
aws rds delete-custom-db-engine-version ^
--engine custom-oracle-ee ^
--engine-version 19.my_cev1
```


Configuring a DB instance for Amazon RDS Custom for Oracle

You can create an RDS Custom DB instance, and then connect to it using Secure Shell (SSH) or AWS Systems Manager.

Topics

- [Overview of Amazon RDS Custom for Oracle architecture \(p. 807\)](#)
- [Creating an RDS Custom for Oracle DB instance \(p. 808\)](#)
- [RDS Custom service-linked role \(p. 812\)](#)
- [Connecting to your RDS Custom DB instance using SSH \(p. 812\)](#)
- [Connecting to your RDS Custom DB instance using AWS Systems Manager \(p. 814\)](#)

Overview of Amazon RDS Custom for Oracle architecture

If you create an Amazon RDS Custom for Oracle DB instance with the Oracle Multitenant architecture (custom-oracle-ee-cdb engine type), your database is a container database (CDB). If you don't specify the Oracle Multitenant architecture, your database is a traditional non-CDB that uses the custom-oracle-ee engine type. A non-CDB can't contain pluggable databases (PDBs).

An RDS Custom for Oracle CDB supports the following features:

- Backups
- Restoring and point-time-restore (PITR) from backups
- Read replicas
- Minor version upgrades

When you create a CDB instance using the Oracle Multitenant architecture, your CDB includes the following:

- CDB root (CDB\$ROOT)
- PDB seed (PDB\$SEED)
- PDB

By default, your CDB is named RDSCDB, which is also the name of the Oracle System ID (Oracle SID), and your PDB is named ORCL. You can choose a different name for your PDB, but the Oracle SID and the PDB name can't be the same.

If you want additional PDBs, create them manually using Oracle SQL. RDS Custom for Oracle doesn't restrict the number of PDBs that you can create using Oracle SQL. RDS Custom for Oracle doesn't supply APIs for PDBs. In general, you are responsible for creating and managing PDBs, as in an on-premises deployment.

Note

If you create a PDB, we recommend that you take a manual snapshot afterward in case you need to perform point-in-time recovery (PITR).

You can't rename existing PDBs using Amazon RDS APIs. You also can't rename the CDB using the `modify-db-instance` command.

The open mode for the CDB root is READ WRITE on the primary and MOUNTED on a mounted standby database. RDS Custom for Oracle attempts to open all PDBs when opening the CDB. If RDS Custom for Oracle can't open all PDBs, it issues the event tenant database shutdown.

Creating an RDS Custom for Oracle DB instance

Create an Amazon RDS Custom for Oracle DB instance using either the AWS Management Console or the AWS CLI. The procedure is similar to the procedure for creating an Amazon RDS DB instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

If you included installation parameters in your CEV manifest, then your DB instance uses the Oracle base, Oracle home, and the ID and name of the UNIX/Linux user and group that you specified. The `oratab` file, which is created by Oracle Database during installation, points to the real installation location rather than to a symbolic link. When RDS Custom runs commands, it runs as the configured OS user rather than the default user `rdsdb`. For more information, see [Preparing the CEV manifest \(p. 789\)](#).

Before you attempt to create or connect to an RDS Custom DB instance, complete the tasks in [Setting up your environment for Amazon RDS Custom for Oracle \(p. 768\)](#).

Console

To create an RDS Custom for Oracle DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose **Create database**.
4. In **Choose a database creation method**, select **Standard create**.
5. In **Engine options**, choose **Oracle** for the DB engine type. Oracle Database is the only supported DB engine.
6. For **Database management type**, choose **Amazon RDS Custom**.
7. For **Edition**, choose **Oracle Enterprise Edition**.
8. For **Architecture settings**, choose **Multitenant architecture** if you want your database to be a CDB. At creation, your CDB contains one PDB and one PDB seed. If you don't choose **Multitenant architecture**, your database is a non-CDB, which means it can't contain PDBs.
9. For **Database version**, choose the RDS Custom custom engine version (CEV) that you previously created. The CEV has the following format: *major-engine-version*.*customized_string*. An example identifier is 19.cdb_cev1.

If you chose **Multitenant architecture** in the previous step, you can only specify a Multitenant CEV. The console filters out CEVs that were created as non-CDBs.

10. In **Templates**, choose **Production**.
11. In **Settings**, enter a unique name for the **DB instance identifier**.
12. Enter your master password by doing the following:
 - a. In the **Settings** section, open **Credential Settings**.
 - b. Clear the **Auto generate a password** check box.
 - c. Change the **Master username** value and enter the same password in **Master password** and **Confirm password**. By default, the new RDS Custom DB instance uses an automatically generated password for the master user.

When you connect to a non-CDB, the master user is the user for the non-CDB. When you connect to a CDB, the master user is the user for the PDB. To connect to the CDB root, log in to the host, start a SQL client, and create an administrative user with SQL commands.

13. In **DB instance size**, choose a **DB instance class**.

For supported classes, see [DB instance class support for RDS Custom for Oracle \(p. 766\)](#).

14. Choose **Storage** settings.
15. For **RDS Custom security**, do the following:
 - a. For **IAM instance profile**, choose the instance profile for your RDS Custom for Oracle DB instance.

The IAM instance profile must begin with AWSRDSCustom, for example *AWSRDSCustomInstanceProfileForRdsCustomInstance*.
 - b. For **Encryption**, choose **Enter a key ARN** to list the available AWS KMS keys. Then choose your key from the list.

An AWS KMS key is required for RDS Custom. For more information, see [Make sure that you have a symmetric encryption AWS KMS key \(p. 768\)](#).
16. (Optional) Choose **Add new tag** to apply an identifier to this DB instance.

Important

You can tag RDS Custom DB instances when you create them, but don't create or modify the AWSRDSCustom tag that's required for RDS Custom automation. For more information, see [Tagging RDS Custom for Oracle resources \(p. 824\)](#).

17. For **Initial database name**, enter a name or leave the default value ORCL. In Oracle Multitenant, the initial database name is the PDB name.
18. For the remaining sections, specify your preferred RDS Custom DB instance settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#). The following settings don't appear in the console and aren't supported:

- **Processor features**
- **Storage autoscaling**
- **Availability & durability**
- **Password and Kerberos authentication** option in **Database authentication** (only **Password authentication** is supported)
- **Database options** group in **Additional configuration**
- **Performance Insights**
- **Log exports**
- **Enable auto minor version upgrade**
- **Deletion protection**

Backup retention period is supported, but you can't choose **0 days**.

19. Choose **Create database**.

Important

When you create an RDS Custom for Oracle DB instance, you might receive the following error: The service-linked role is in the process of being created. Try again later. If you do, wait a few minutes and then try again to create the DB instance.

The **View credential details** button appears on the **Databases** page.

To view the master user name and password for the RDS Custom DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it. If you need to change the master user password after the RDS Custom DB instance is available, modify the DB instance to do so. For more information about modifying a DB instance, see [Managing an Amazon RDS Custom for Oracle DB instance \(p. 816\)](#).

20. Choose **Databases** to view the list of RDS Custom DB instances.
21. Choose the RDS Custom DB instance that you just created.

On the RDS console, the details for the new RDS Custom DB instance appear:

- The DB instance has a status of **creating** until the RDS Custom DB instance is created and ready for use. When the state changes to **available**, you can connect to the DB instance. Depending on the instance class and storage allocated, it can take several minutes for the new DB instance to be available.
- **Role** has the value **Instance (RDS Custom)**.
- **RDS Custom automation mode** has the value **Full automation**. This setting means that the DB instance provides automatic monitoring and instance recovery.

AWS CLI

You create an RDS Custom DB instance by using the `create-db-instance` AWS CLI command.

The following options are required:

- `--db-instance-identifier`
- `--db-instance-class` (for a list of supported instance classes, see [DB instance class support for RDS Custom for Oracle \(p. 766\)](#))
- `--engine engine_type` (where `engine-type` is `custom-oracle-ee-cdb` for a CDB and `custom-oracle-ee` for a non-CDB)
- `--engine-version cev` (where `cev` is the name of the custom engine version that you specified in [Creating a CEV \(p. 798\)](#))
- `--kms-key-id`
- `--no-auto-minor-version-upgrade`
- `--custom-iam-instance-profile`

The following example creates an RDS Custom DB instance named `my-cdb-instance`. The database is a CDB. The PDB name is `my-pdb`. The backup retention period is three days.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
  --engine custom-oracle-ee-cdb \
  --db-instance-identifier my-cdb-instance \
  --engine-version 19.cdb_cev1 \
  --db-name my-pdb \
  --allocated-storage 250 \
  --db-instance-class db.m5.xlarge \
  --db-subnet-group mydbsubnetgroup \
  --master-username myawsuser \
  --master-user-password mypassword \
```

```
--backup-retention-period 3 \
--no-multi-az \
--port 8200 \
--license-model bring-your-own-license \
--kms-key-id my-kms-key \
--no-auto-minor-version-upgrade \
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

For Windows:

```
aws rds create-db-instance ^
--engine custom-oracle-ee-cdb ^
--db-instance-identifier my-cdb-instance ^
--engine-version 19.cdb_cev1 ^
--db-name my-pdb ^
--allocated-storage 250 ^
--db-instance-class db.m5.xlarge ^
--db-subnet-group mydbsubnetgroup ^
--master-username myawsuser ^
--master-user-password mypassword ^
--backup-retention-period 3 ^
--no-multi-az ^
--port 8200 ^
--license-model bring-your-own-license ^
--kms-key-id my-kms-key ^
--no-auto-minor-version-upgrade ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

Get details about your instance by using the describe-db-instances command.

Example

```
aws rds describe-db-instances --db-instance-identifier my-cdb-instance
```

The following partial output shows the engine, parameter groups, and other information.

```
{
    "DBInstances": [
        {
            "PendingModifiedValues": {},
            "Engine": "custom-oracle-ee-cdb",
            "MultiAZ": false,
            "DBSecurityGroups": [],
            "DBParameterGroups": [
                {
                    "DBParameterGroupName": "default.custom-oracle-ee-cdb-19",
                    "ParameterApplyStatus": "in-sync"
                }
            ],
            "AutomationMode": "full",
            "DBInstanceIdentifier": "my-cdb-instance",
            ...
            "TagList": [
                {
                    "Key": "AWSRDSCustom",
                    "Value": "custom-oracle"
                }
            ]
        }
    ]
}
```

RDS Custom service-linked role

A *service-linked role* gives Amazon RDS Custom access to resources in your AWS account. It makes using RDS Custom easier because you don't have to manually add the necessary permissions. RDS Custom defines the permissions of its service-linked roles, and unless defined otherwise, only RDS Custom can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy can't be attached to any other IAM entity.

When you create an RDS Custom DB instance, both the Amazon RDS and RDS Custom service-linked roles are created (if they don't already exist) and used. For more information, see [Using service-linked roles for Amazon RDS \(p. 2089\)](#).

The first time that you create an RDS Custom for Oracle DB instance, you might receive the following error: The service-linked role is in the process of being created. Try again later. If you do, wait a few minutes and then try again to create the DB instance.

Connecting to your RDS Custom DB instance using SSH

After you create your RDS Custom DB instance, you can connect to this instance using an SSH client. The procedure is the same as for connecting to an Amazon EC2 instance. For more information, see [Connecting to your Linux instance using SSH](#).

To connect to the DB instance, you need the key pair associated with the instance. RDS Custom creates the key pair on your behalf. The pair name uses the prefix `do-not-delete-rds-custom-ssh-privatekey-db-`. AWS Secrets Manager stores your private key as a secret.

Complete the task in the following steps:

1. [Configure your DB instance to allow SSH connections \(p. 812\)](#)
2. [Retrieve your secret key \(p. 812\)](#)
3. [Connect to your EC2 instance using the ssh utility \(p. 814\)](#)

Configure your DB instance to allow SSH connections

Make sure that your DB instance security group permits inbound connections on port 22 for TCP. To learn how to configure your instance security group, see [Configure your instance security group \(p. 775\)](#).

Retrieve your secret key

Retrieve the secret key using either AWS Management Console or the AWS CLI.

Console

To retrieve the secret key

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance to which you want to connect.
3. Choose **Configuration**.
4. Note the **Resource ID** value. For example, the resource ID might be `db-ABCDEFGHijklmn0PQRS0123456`.
5. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
6. In the navigation pane, choose **Instances**.

7. Find the name of your EC2 instance, and choose the instance ID associated with it. For example, the EC2 instance ID might be i-abcdefgijklm01234.
8. In **Details**, find **Key pair name**. The pair name includes the resource ID. For example, the pair name might be do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.
9. In the instance summary, find **Public IPv4 DNS**. For the example, the public Domain Name System (DNS) address might be ec2-12-345-678-901.us-east-2.compute.amazonaws.com.
10. Open the AWS Secrets Manager console at <https://console.aws.amazon.com/secretsmanager/>.
11. Choose the secret that has the same name as your key pair.
12. Choose **Retrieve secret value**.
13. Copy the private key into a text file, and then save the file with the .pem extension. For example, save the file as /tmp/do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem.

AWS CLI

To retrieve the private key, use the AWS CLI.

Example

To find the DB resource ID of your RDS Custom DB instance, use aws rds describe-db-instances.

```
aws rds describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
    --output text
```

The following sample output shows the resource ID for your RDS Custom instance. The prefix is db-.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

To find the EC2 instance ID of your DB instance, use aws ec2 describe-instances. The following example uses db-ABCDEFGHIJKLMNOPQRS0123456 for the resource ID.

```
aws ec2 describe-instances \
    --filters "Name>tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
    --output text \
    --query 'Reservations[*].Instances[*].InstanceId'
```

The following sample output shows the EC2 instance ID.

```
i-abcdefgijklm01234
```

To find the key name, specify the EC2 instance ID.

```
aws ec2 describe-instances \
    --instance-ids i-0bdc4219e66944afa \
    --output text \
    --query 'Reservations[*].Instances[*].KeyName'
```

The following sample output shows the key name, which uses the prefix do-not-delete-rds-custom-ssh-privatekey-.

```
do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c
```

To save the private key in a .pem file named after the key, use aws secretsmanager. The following example saves the file in your /tmp directory.

```
aws secretsmanager get-secret-value \
--secret-id do-not-delete-rds-custom-ssh-privatekey-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c \
--query SecretString \
--output text >/tmp/do-not-delete-rds-custom-ssh-privatekey-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem
```

Connect to your EC2 instance using the ssh utility

The following example assumes that you created a .pem file that contains your private key.

Change to the directory that contains your .pem file. Using chmod, set the permissions to 400.

```
cd /tmp
chmod 400 do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem
```

To obtain your public DNS name, use the command ec2 describe-instances.

```
aws ec2 describe-instances \
--instance-ids i-abcdefhijklm01234 \
--output text \
--query 'Reservations[*].Instances[*].PublicDnsName'
```

The following sample output shows the public DNS name.

```
ec2-12-345-678-901.us-east-2.compute.amazonaws.com
```

In the ssh utility, specify the .pem file and the public DNS name of the instance.

```
ssh -i \
"do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem" \
ec2-user@ec2-12-345-678-901.us-east-2.compute.amazonaws.com
```

Connecting to your RDS Custom DB instance using AWS Systems Manager

After you create your RDS Custom DB instance, you can connect to it using AWS Systems Manager Session Manager. Session Manager is an Systems Manager capability that you can use to manage Amazon EC2 instances through a browser-based shell or through the AWS CLI. For more information, see [AWS Systems Manager Session Manager](#).

Console

To connect to your DB instance using Session Manager

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance to which you want to connect.
3. Choose **Configuration**.
4. Note the **Resource ID** for your DB instance. For example, the resource ID might be db-ABCDEFGHIJKLMNOPQRS0123456.

5. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
6. In the navigation pane, choose **Instances**.
7. Look for the name of your EC2 instance, and then click the instance ID associated with it. For example, the instance ID might be i-abcdefgijklm01234.
8. Choose **Connect**.
9. Choose **Session Manager**.
10. Choose **Connect**.

A window opens for your session.

AWS CLI

You can connect to your RDS Custom DB instance using the AWS CLI. This technique requires the Session Manager plugin for the AWS CLI. To learn how to install the plugin, see [Install the Session Manager plugin for the AWS CLI](#).

To find the DB resource ID of your RDS Custom DB instance, use `aws rds describe-db-instances`.

```
aws rds describe-db-instances \
--query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
--output text
```

The following sample output shows the resource ID for your RDS Custom instance. The prefix is db-.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

To find the EC2 instance ID of your DB instance, use `aws ec2 describe-instances`. The following example uses db-ABCDEFGHIJKLMNOPQRS0123456 for the resource ID.

```
aws ec2 describe-instances \
--filters "Name>tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
--output text \
--query 'Reservations[*].Instances[*].InstanceId'
```

The following sample output shows the EC2 instance ID.

```
i-abcdefgijklm01234
```

Use the `aws ssm start-session` command, supplying the EC2 instance ID in the `--target` parameter.

```
aws ssm start-session --target "i-abcdefgijklm01234"
```

A successful connection looks like the following.

```
Starting session with SessionId: yourid-abcdefgijklm1234
[ssm-user@ip-123-45-67-89 bin]$
```

Managing an Amazon RDS Custom for Oracle DB instance

Amazon RDS Custom supports a subset of the usual management tasks for Amazon RDS DB instances. Following, you can find instructions for the supported RDS Custom for Oracle management tasks using the AWS Management Console and the AWS CLI.

Topics

- [Working with container databases \(CDBs\) in RDS Custom for Oracle \(p. 816\)](#)
- [Working with high availability features for RDS Custom for Oracle \(p. 817\)](#)
- [Pausing and resuming RDS Custom automation \(p. 817\)](#)
- [Modifying the storage for an RDS Custom for Oracle DB instance \(p. 820\)](#)
- [Changing the time zone of an RDS Custom for Oracle DB instance \(p. 822\)](#)
- [Changing the character set of an RDS Custom for Oracle DB instance \(p. 823\)](#)
- [Support for Transparent Data Encryption \(p. 824\)](#)
- [Tagging RDS Custom for Oracle resources \(p. 824\)](#)
- [Deleting an RDS Custom for Oracle DB instance \(p. 824\)](#)

Working with container databases (CDBs) in RDS Custom for Oracle

You can either create your RDS Custom for Oracle DB instance with the Oracle Multitenant architecture (custom-oracle-ee-cdb engine type) or with the traditional non-CDB architecture (custom-oracle-ee engine type). When you create a container database (CDB), it contains one pluggable database (PDB) and one PDB seed. You can create additional PDBs manually using Oracle SQL.

In the RDS Custom for Oracle shared responsibility model, you are responsible for managing PDBs and creating any additional PDBs. RDS Custom doesn't restrict the number of PDBs. You can manually create, modify, and delete PDBs by connecting to the CDB root and running a SQL command. Create PDBs on an Amazon EBS data volume to prevent the DB instance from going outside the support perimeter.

You can't rename existing PDBs using Amazon RDS APIs. You also can't rename the CDB using the `modify-db-instance` command.

To modify your CDBs or PDBs, complete the following steps:

1. Pause automation to prevent interference with RDS Custom actions.
2. Modify your CDB or PDBs.
3. Back up any modified PDBs.
4. Resume automation.

RDS Custom keeps the CDB root open in the same way as it keeps a non-CDB open. If the state of the CDB root changes, the monitoring and recovery automation attempts to recover the CDB root to the desired state. You receive RDS event notifications when the root CDB is shut down (RDS-EVENT-0004) or restarted (RDS-EVENT-0006), similar to the non-CDB architecture. RDS Custom attempts to open all PDBs in READ WRITE mode at DB instance startup. If some PDBs can't be opened, RDS Custom publishes the following event: tenant database shutdown.

Working with high availability features for RDS Custom for Oracle

To support replication between RDS Custom for Oracle instances, you can configure high availability (HA) with Oracle Data Guard. The primary DB instance automatically synchronizes data to the standby instances.

You can configure your high availability environment in the following ways:

- Configure standby instances in different Availability Zones (AZs) to be resilient to AZ failures.
- Place your standby databases in mounted or read-only mode.
- Fail over or switch over from the primary database to a standby database with no data loss.
- Migrate data by configuring high availability for your on-premises instance, and then failing over or switching over to the RDS Custom standby database.

To learn how to configure high availability, see the whitepaper [Build high availability for Amazon RDS Custom for Oracle using read replicas](#). You can perform the following tasks:

- Use a virtual private network (VPN) tunnel to encrypt data in transit for your high availability instances. Encryption in transit isn't configured automatically by RDS Custom.
- Configure Oracle Fast-Failover Observer (FSFO) to monitor your high availability instances.
- Allow the observer to perform automatic failover when necessary conditions are met.

Pausing and resuming RDS Custom automation

RDS Custom automatically provides monitoring and instance recovery for an RDS Custom for Oracle DB instance. If you need to customize your DB instance, do the following:

1. Pause RDS Custom automation for a specified period. The pause ensures that your customizations don't interfere with RDS Custom automation.
2. Customize the RDS Custom for Oracle DB instance as needed.
3. Do either of the following:
 - Resume automation manually.

Important

Pausing and resuming automation are the only supported automation tasks when modifying an RDS Custom for Oracle DB instance.

- Wait for the pause period to end. In this case, RDS Custom resumes monitoring and instance recovery automatically.

In an on-premises Oracle CDB, you can preserve a specified open mode for PDBs using a built-in command or after a startup trigger. This mechanism brings PDBs to a specified state when the CDB restarts. When opening your CDB, RDS Custom automation always discards any user-specified preserved states and attempts to open all PDBs. If RDS Custom can't open all PDBs, the following event is issued: The following PDBs failed to open: *list-of-PDBs*.

Console

To pause or resume RDS Custom automation

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **RDS Custom automation mode**, choose one of the following options:
 - **Paused** pauses the monitoring and instance recovery for the RDS Custom DB instance. Enter the pause duration that you want (in minutes) for **Automation mode duration**. The minimum value is 60 minutes (default). The maximum value is 1,440 minutes.
 - **Full automation** resumes automation.
5. Choose **Continue** to check the summary of modifications.

A message indicates that RDS Custom will apply the changes immediately.
6. If your changes are correct, choose **Modify DB instance**. Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

On the RDS console, the details for the modification appear. If you paused automation, the **Status** of your RDS Custom DB instance indicates **Automation paused**.
7. (Optional) In the navigation pane, choose **Databases**, and then your RDS Custom DB instance.

In the **Summary** pane, **RDS Custom automation mode** indicates the automation status. If automation is paused, the value is **Paused**. **Automation resumes in *num* minutes**.

AWS CLI

To pause or resume RDS Custom automation, use the [modify-db-instance](#) AWS CLI command. Identify the DB instance using the required parameter `--db-instance-identifier`. Control the automation mode with the following parameters:

- `--automation-mode` specifies the pause state of the DB instance. Valid values are `all-paused`, which pauses automation, and `full`, which resumes it.
- `--resume-full-automation-mode-minutes` specifies the duration of the pause. The default value is 60 minutes.

Note

Regardless of whether you specify `--no-apply-immediately` or `--apply-immediately`, RDS Custom applies modifications asynchronously as soon as possible.

In the command response, `ResumeFullAutomationModeTime` indicates the resume time as a UTC timestamp. When the automation mode is `all-paused`, you can use `modify-db-instance` to resume automation mode or extend the pause period. No other `modify-db-instance` options are supported.

The following example pauses automation for `my-custom-instance` for 90 minutes.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --automation-mode all-paused \
  --resume-full-automation-mode-minutes 90
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier my-custom-instance ^
```

```
--automation-mode all-paused ^
--resume-full-automation-mode-minutes 90
```

The following example extends the pause duration for an extra 30 minutes. The 30 minutes is added to the original time shown in ResumeFullAutomationModeTime.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier my-custom-instance \
--automation-mode all-paused \
--resume-full-automation-mode-minutes 30
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier my-custom-instance ^
--automation-mode all-paused ^
--resume-full-automation-mode-minutes 30
```

The following example resumes full automation for my-custom-instance.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier my-custom-instance \
--automation-mode full \
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier my-custom-instance ^
--automation-mode full
```

In the following partial sample output, the pending AutomationMode value is full.

```
{
    "DBInstance": {
        "PubliclyAccessible": true,
        "MasterUsername": "admin",
        "MonitoringInterval": 0,
        "LicenseModel": "bring-your-own-license",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "0123456789abcdefg"
            }
        ],
        "InstanceCreateTime": "2020-11-07T19:50:06.193Z",
        "CopyTagsToSnapshot": false,
        "OptionGroupMemberships": [
            {
                "Status": "in-sync",
                "OptionGroupName": "default:custom-oracle-ee-19"
            }
        ],
    }
}
```

```

    "PendingModifiedValues": {
        "AutomationMode": "full"
    },
    "Engine": "custom-oracle-ee",
    "MultiAZ": false,
    "DBSecurityGroups": [],
    "DBParameterGroups": [
        {
            "DBParameterGroupName": "default.custom-oracle-ee-19",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    ...
    "ReadReplicaDBInstanceIdentifiers": [],
    "AllocatedStorage": 250,
    "DBInstanceArn": "arn:aws:rds:us-west-2:012345678912:db:my-custom-instance",
    "BackupRetentionPeriod": 3,
    "DBName": "ORCL",
    "PreferredMaintenanceWindow": "fri:10:56-fri:11:26",
    "Endpoint": {
        "HostedZoneId": "ABCDEFGHIJKLMNO",
        "Port": 8200,
        "Address": "my-custom-instance.abcdefghijkl.us-west-2.rds.amazonaws.com"
    },
    "DBInstanceState": "automation-paused",
    "IAMDatabaseAuthenticationEnabled": false,
    "AutomationMode": "all-paused",
    "EngineVersion": "19.my_cev1",
    "DeletionProtection": false,
    "AvailabilityZone": "us-west-2a",
    "DomainMemberships": [],
    "StorageType": "gp2",
    "DbiResourceId": "db-ABCDEFGHIJKLMN0PQRSTUVWXYZ",
    "ResumeFullAutomationModeTime": "2020-11-07T20:56:50.565Z",
    "KmsKeyId": "arn:aws:kms:us-west-2:012345678912:key/
aa111a11-111a-11a1-1a11-1111a11a1a1a",
        "StorageEncrypted": false,
        "AssociatedRoles": [],
        "DBInstanceClass": "db.m5.xlarge",
        "DbInstancePort": 0,
        "DBIdentifier": "my-custom-instance",
        "TagList": []
    }
}

```

Modifying the storage for an RDS Custom for Oracle DB instance

Modifying storage for an RDS Custom for Oracle DB instance is similar to modifying storage for an Amazon RDS DB instance, but you can only do the following:

- Increase the allocated storage.
- Change the storage type from io1 to gp2, or gp2 to io1.
- Change the Provisioned IOPS, if you're using the io1 storage type.

The following limitations apply to modifying the storage for an RDS Custom for Oracle DB instance:

- The minimum allocated storage for RDS Custom for Oracle is 40 GiB, and the maximum is 64 TiB.
- As with Amazon RDS, you can't decrease the allocated storage. This is a limitation of Amazon EBS volumes.
- Storage autoscaling isn't supported for RDS Custom DB instances.

- Any storage volumes that you attach manually to your RDS Custom DB instance are outside the support perimeter.

For more information, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

- Magnetic (standard) storage isn't supported for RDS Custom.

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

For general information about storage modification, see [Working with storage for Amazon RDS DB instances \(p. 410\)](#). The following procedures are specific to RDS Custom.

Console

To modify the storage for an RDS Custom for Oracle DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify.
4. Choose **Modify**.
5. Make the following changes as needed:
 - a. Enter a new value for **Allocated storage**. It must be greater than the current value, and from 40 GiB–64 TiB.
 - b. Change the value for **Storage type**. You can use General Purpose (gp2) or Provisioned IOPS (io1) storage.
 - c. If using io1 storage, you can change the **Provisioned IOPS** value.
6. Choose **Continue**.
7. Choose **Apply immediately** or **Apply during the next scheduled maintenance window**.
8. Choose **Modify DB instance**.

AWS CLI

To modify the storage for an RDS Custom for Oracle DB instance, use the [modify-db-instance](#) AWS CLI command. Set the following parameters as needed:

- **--allocated-storage** – Amount of storage to be allocated for the DB instance, in gibibytes. It must be greater than the current value, and from 40–65,536 GiB.
- **--storage-type** – The storage type, gp2 or io1.
- **--iops** – Provisioned IOPS for the DB instance, if using the io1 storage type.
- **--apply-immediately** – Use **--apply-immediately** to apply the storage changes immediately.
Or use **--no-apply-immediately** (the default) to apply the changes during the next maintenance window.

The following example changes the storage size of my-custom-instance to 200 GiB, storage type to io1, and Provisioned IOPS to 3000.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
```

```
--db-instance-identifier my-custom-instance \
--storage-type io1 \
--iops 3000 \
--allocated-storage 200 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier my-custom-instance ^
--storage-type io1 ^
--iops 3000 ^
--allocated-storage 200 ^
--apply-immediately
```

Changing the time zone of an RDS Custom for Oracle DB instance

You change the time zone of an RDS Custom for Oracle DB instance manually. This approach contrasts with RDS for Oracle, where you use the `TIME_ZONE` option in a custom DB option group.

You can change time zones for RDS Custom for Oracle DB instances multiple times. However, we recommend not changing them more than once every 48 hours. We also recommend changing them only when the latest restorable time is within the last 30 minutes.

If you don't follow these recommendations, cleaning up redo logs might remove more logs than intended. Redo log timestamps might also be converted incorrectly to UTC, which can prevent the redo log files from being downloaded and replayed correctly. This in turn can prevent point-in-time recovery (PITR) from performing correctly.

Changing the time zone of an RDS Custom for Oracle DB instance has the following limitations:

- PITR is supported for recovery times before RDS Custom automation is paused, and after automation is resumed.

For more information about PITR, see [Restoring an RDS Custom for Oracle instance to a point in time \(p. 833\)](#).
- Changing the time zone of an existing read replica causes downtime. We recommend changing the time zone of the DB instance before creating read replicas.

You can create a read replica from a DB instance with a modified time zone. For more information about read replicas, see [Working with Oracle replicas for RDS Custom for Oracle \(p. 826\)](#).

Use the following procedures to change the time zone of an RDS Custom for Oracle DB instance.

Make sure to follow these procedures. If they aren't followed, it can result in these issues:

- Disruption of redo log download and replay
- Incorrect redo log timestamps
- Cleanup of redo logs on the host that doesn't use the redo log retention period

To change the time zone for a primary DB instance

1. Pause RDS Custom automation. For more information, see [Pausing and resuming RDS Custom automation \(p. 817\)](#).
2. (Optional) Change the time zone of the DB instance, for example by using the following command.

```
ALTER DATABASE SET TIME_ZONE = 'US/Pacific';
```

3. Shut down the DB instance.
4. Log in to the host and change the system time zone.
5. Start the DB instance.
6. Resume RDS Custom automation.

To change the time zone for a primary DB instance and its read replicas

1. Pause RDS Custom automation on the primary DB instance.
2. Pause RDS Custom automation on the read replicas.
3. (Optional) Change the time zone of the primary and read replicas, for example by using the following command.

```
ALTER DATABASE SET TIME_ZONE = 'US/Pacific';
```

4. Shut down the primary DB instance.
5. Shut down the read replicas.
6. Log in to the host and change the system time zone for the read replicas.
7. Change the system time zone for the primary DB instance.
8. Mount the read replicas.
9. Start the primary DB instance.
10. Resume RDS Custom automation on the primary DB instance and then on the read replicas.

Changing the character set of an RDS Custom for Oracle DB instance

RDS Custom for Oracle defaults to the character set US7ASCII. You might want to specify different character sets to meet language or multibyte character requirements. When you use RDS Custom for Oracle, you can pause automation and then change the character set of your database manually.

Changing the character set of an RDS Custom for Oracle DB instance has the following requirements:

- You can only change the character set on a newly provisioned RDS Custom instance that has an empty or starter database with no application data. For all other scenarios, change the character set using DMU (Database Migration Assistant for Unicode).
- You can only change to a character set supported by RDS for Oracle. For more information, see [Supported DB character sets \(p. 1483\)](#).

To change the character set of an RDS Custom for Oracle DB instance

1. Pause RDS Custom automation. For more information, see [Pausing and resuming RDS Custom automation \(p. 817\)](#).
2. Log in to your database as a user with SYSDBA privileges.
3. Restart the database in restricted mode, change the character set, and then restart the database in normal mode.

Run the following script in your SQL client:

```
SHUTDOWN IMMEDIATE;
```

```
STARTUP RESTRICT;
ALTER DATABASE CHARACTER SET INTERNAL_CONVERT AL32UTF8;
SHUTDOWN IMMEDIATE;
STARTUP;
SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER = 'NLS_CHARACTERSET';
```

Verify that the output shows the correct character set:

```
VALUE
-----
AL32UTF8
```

4. Resume RDS Custom automation. For more information, see [Pausing and resuming RDS Custom automation \(p. 817\)](#).

Support for Transparent Data Encryption

RDS Custom supports Transparent Data Encryption (TDE) for RDS Custom for Oracle DB instances.

However, you can't enable TDE using an option in a custom option group as you can in RDS for Oracle. You turn on TDE manually. For information about using Oracle Transparent Data Encryption, see [Securing stored data using Transparent Data Encryption](#) in the Oracle documentation.

Tagging RDS Custom for Oracle resources

You can tag RDS Custom resources as with Amazon RDS resources, but with some important differences:

- Don't create or modify the AWSRDSCustom tag that's required for RDS Custom automation. If you do, you might break the automation.
- Tags added to RDS Custom DB instances during creation are propagated to all other related RDS Custom resources.
- Tags aren't propagated when you add them to RDS Custom resources after DB instance creation.

For general information about resource tagging, see [Tagging Amazon RDS resources \(p. 392\)](#).

Deleting an RDS Custom for Oracle DB instance

To delete an RDS Custom DB instance, do the following:

- Provide the name of the DB instance.
- Clear the option to take a final DB snapshot of the DB instance.
- Choose or clear the option to retain automated backups.

You can delete an RDS Custom DB instance using the console or the CLI. The time required to delete the DB instance can vary depending on the backup retention period (that is, how many backups to delete) and how much data is deleted.

Console

To delete an RDS Custom DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance that you want to delete. RDS Custom DB instances show the role **Instance (RDS Custom)**.

3. For **Actions**, choose **Delete**.
4. To retain automated backups, choose **Retain automated backups**.
5. Enter **delete me** in the box.
6. Choose **Delete**.

AWS CLI

You delete an RDS Custom DB instance by using the `delete-db-instance` AWS CLI command. Identify the DB instance using the required parameter `--db-instance-identifier`. The remaining parameters are the same as for an Amazon RDS DB instance, with the following exceptions:

- `--skip-final-snapshot` is required.
- `--no-skip-final-snapshot` isn't supported.
- `--final-db-snapshot-identifier` isn't supported.

The following example deletes the RDS Custom DB instance named `my-custom-instance`, and retains automated backups.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \
  --db-instance-identifier my-custom-instance \
  --skip-final-snapshot \
  --no-delete-automated-backups
```

For Windows:

```
aws rds delete-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --skip-final-snapshot ^
  --no-delete-automated-backups
```

Working with Oracle replicas for RDS Custom for Oracle

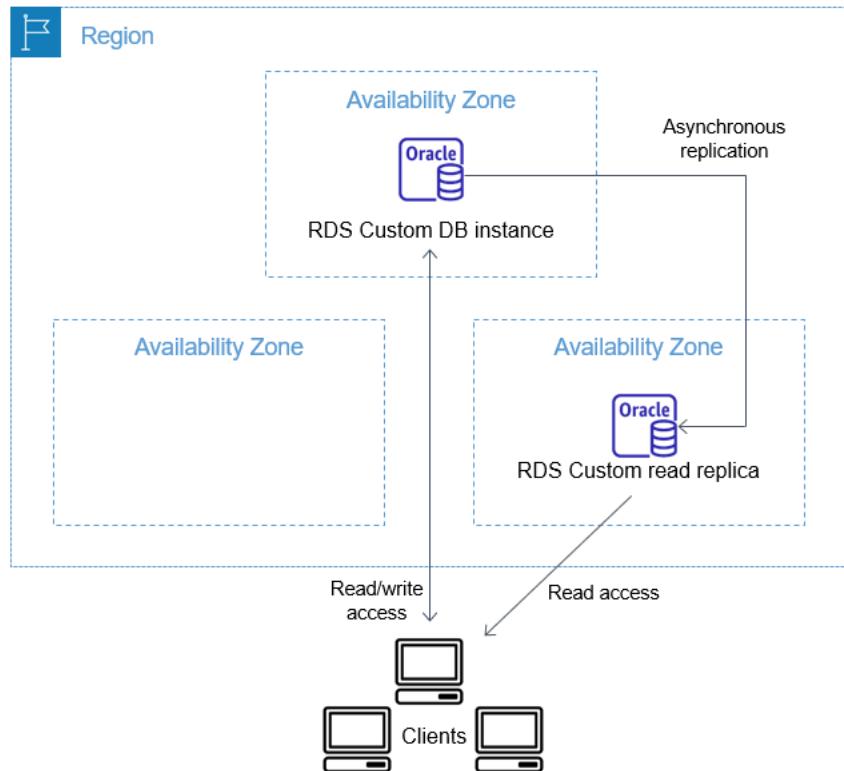
You can create Oracle replicas for RDS Custom for Oracle DB instances. Both container databases (CDBs) and non-CDBs are supported. Creating an Oracle replica is similar to the process in Amazon RDS, but with important differences. For general information about creating and managing Oracle replicas, see [Working with read replicas \(p. 370\)](#) and [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#).

Topics

- [Overview of RDS Custom for Oracle replication \(p. 826\)](#)
- [Requirements and limitations for RDS Custom for Oracle replication \(p. 827\)](#)
- [Promoting an RDS Custom for Oracle replica to a standalone DB instance \(p. 829\)](#)

Overview of RDS Custom for Oracle replication

The architecture of RDS Custom for Oracle replication is analogous to RDS for Oracle replication. A primary DB instance replicates asynchronously to one or more Oracle replicas.



As with RDS for Oracle, you can create up to five managed Oracle replicas of your RDS Custom for Oracle primary DB instance. You can also create your own manually configured (external) Oracle replicas. External replicas don't count toward your instance limit. They also lie outside the RDS Custom support perimeter. For more information about the support perimeter, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

Oracle replica names are based on the database unique name. The format is `DB_UNIQUE_NAME_X`, with letters appended sequentially. For example, if your database unique name is ORCL, the first two replicas are named ORCL_A and ORCL_B. The first six letters, A–F, are reserved for RDS Custom. RDS Custom

copies database parameters from your primary DB instance to the replicas. For more information, see [DB_UNIQUE_NAME](#) in the Oracle documentation.

By default, RDS Custom Oracle replicas use the same backup retention period as your primary DB instance. You can modify the backup retention period to 1–35 days. RDS Custom supports backing up, restoring, and point-in-time recovery (PITR). For more information about backing up and restoring RDS Custom DB instances, see [Backing up and restoring an Amazon RDS Custom for Oracle DB instance \(p. 831\)](#).

You can promote managed Oracle replicas in RDS Custom for Oracle using the console, `promote-read-replica` AWS CLI command, or `PromoteReadReplica` API. If you delete your primary DB instance, and all replicas are healthy, RDS Custom for Oracle promotes your managed replicas to standalone instances automatically. If a replica has paused automation or is outside the support perimeter, you must fix the replica before RDS Custom can promote it automatically. You can only promote external Oracle replicas manually.

Requirements and limitations for RDS Custom for Oracle replication

When you create RDS Custom for Oracle replicas, not all RDS Oracle replica options are supported.

Topics

- [General requirements and limitations \(p. 827\)](#)
- [Networking requirements and limitations \(p. 828\)](#)
- [External replica requirements and limitations \(p. 828\)](#)
- [Replica promotion requirements and limitations \(p. 829\)](#)

General requirements and limitations

RDS Custom for Oracle replicas have the following limitations:

- We recommend that you create Oracle replicas only for RDS Custom for Oracle DB instances created after November 18, 2022. If you need to create Oracle replicas for pre-existing RDS Custom for Oracle DB instances, see [Troubleshooting replica creation for RDS Custom for Oracle \(p. 900\)](#).
- You can create RDS Custom for Oracle replicas in mounted mode only. However, you can manually change the mode of mounted replicas to read-only, and from read-only to mounted. For more information, see the documentation for the `create-db-instance-read-replica` AWS CLI command.
- Cross-Region Oracle replicas aren't supported.
- Make sure not to modify the RDS_DATAGUARD user. This user is reserved for RDS Custom for Oracle automation. Modifying this user can result in undesired outcomes, such as an inability to create Oracle replicas for your RDS Custom for Oracle DB instance.
- You can't change the value of the Oracle Data Guard `CommunicationTimeout` parameter. This parameter is set to 15 seconds for RDS Custom for Oracle DB instances.
- Make sure not to change the replication user password. It is required to administer the Oracle Data Guard configuration on the host. If you change the password, RDS Custom for Oracle might put your Oracle replica outside the support perimeter. For more information, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

The password is stored in AWS Secrets Manager, tagged with the DB resource ID. Each Oracle replica has its own secret in Secrets Manager. The format for the secret is the following.

```
do-not-delete-rds-custom-db-DB_resource_id-6-digit_UUID-dg
```

- While creating a Oracle replica, RDS Custom temporarily pauses the cleanup of redo log files. In this way, RDS Custom ensures that it can apply these logs to the new Oracle replica after it becomes available.
- If your RDS Custom DB instance is a CDB, we recommend that you don't specify the clause STANDBYS=NONE in a CREATE PLUGGABLE DATABASE command. The goal is to ensure that your standby CDB contains all PDBs if a failover occurs.

Networking requirements and limitations

Make sure that your network configuration supports RDS Custom for Oracle replicas. Consider the following requirements and limitations:

- Make sure to enable port 1140 for both inbound and outbound communication within your virtual private cloud (VPC) for the primary DB instance and all of the replicas. This is required for Oracle Data Guard communication between the read replicas.
- RDS Custom for Oracle validates the network while creating a Oracle replica. If the primary DB instance and the new replica can't connect over the network, RDS Custom for Oracle doesn't create the replica and places it in the INCOMPATIBLE_NETWORK state.
- For external Oracle replicas, such as those you create on Amazon EC2 or on-premises, use another port and listener for Oracle Data Guard replication. Trying to use port 1140 could cause conflicts with RDS Custom automation.
- The /rdsdbdata/config/tnsnames.ora file contains network service names mapped to listener protocol addresses. Note the following requirements and recommendations:
 - Entries in tnsnames.ora prefixed with rds_custom_ are reserved for RDS Custom when handling Oracle replica operations.

When creating manual entries in tnsnames.ora, don't use this prefix.

- In some cases, you might want to switch over or fail over manually, or use failover technologies such as Fast-Start Failover (FSFO). If so, make sure to manually synchronize tnsnames.ora entries from the primary DB instance to all of the standby instances. This recommendation applies to both Oracle replicas managed by RDS Custom and to external Oracle replicas.

RDS Custom automation updates tnsnames.ora entries on only the primary DB instance. Make sure also to synchronize when you add or remove a Oracle replica.

If you don't synchronize the tnsnames.ora files and switch over or fail over manually, Oracle Data Guard on the primary DB instance might not be able to communicate with the Oracle replicas.

External replica requirements and limitations

RDS Custom for Oracle external replicas, which include on-premises replicas, have the following limitations:

- RDS Custom for Oracle detects instance role changes upon manual failover, such as FSFO, for managed Oracle replicas but not for external Oracle replicas.

The role change is noted in the event log. You can also see the new state by using the [describe-db-instances](#) AWS CLI command.

- RDS Custom for Oracle detects high replication lag for managed Oracle replicas but not for external Oracle replicas.

High replication lag produces the Replication has stopped event. You can also see the replication status by using the [describe-db-instances](#) AWS CLI command, but there might be a delay for it to be updated.

- RDS Custom for Oracle doesn't promote external Oracle replicas automatically after you delete your primary DB instance. The automatic promotion feature is available only for managed Oracle replicas. For information about promoting Oracle replicas manually, see the white paper [Enabling high availability with Data Guard on Amazon RDS Custom for Oracle](#).

Replica promotion requirements and limitations

Promoting RDS Custom for Oracle managed Oracle replicas is the same as promoting RDS managed replicas, with some differences. Note the following requirements and limitations for RDS Custom for Oracle:

- You can't promote a replica while RDS Custom for Oracle is backing it up.
- When you promote your Oracle replica, you can't change the backup retention period to 0.
- Make sure not to initiate a failover while RDS Custom for Oracle is promoting your replica. Otherwise, the promotion workflow could become stuck.
- Make sure not to switch over your primary DB instance while RDS Custom for Oracle is promoting your Oracle replica. Otherwise, the promotion workflow could become stuck.
- Make sure not to shut down your primary DB instance while RDS Custom for Oracle is promoting your Oracle replica. Otherwise, the promotion workflow could become stuck.
- Make sure not to attempt to restart replication with your newly promoted DB instance as a target. After RDS Custom for Oracle promotes your Oracle replica, it becomes a standalone DB instance and no longer has the replica role.
- If you issue `delete-db-instance` on the primary DB instance, RDS Custom for Oracle validates that each managed Oracle replica is healthy and available for promotion. A replica might be ineligible for promotion because automation is paused or it is outside the support perimeter. In such cases, RDS Custom for Oracle publishes an event explaining the issue so that you can repair your Oracle replica manually.
- If you maintain external Oracle replicas and delete your primary DB instance, you must promote your external Oracle replicas manually.

For more information, see [Troubleshooting replica promotion for RDS Custom for Oracle \(p. 900\)](#).

Promoting an RDS Custom for Oracle replica to a standalone DB instance

Just as with RDS for Oracle, you can promote an RDS Custom for Oracle replica to a standalone DB instance. When you promote a Oracle replica, RDS Custom for Oracle reboots the DB instance before it becomes available. For more information about promoting Oracle replicas, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

The following steps show the general process for promoting a Oracle replica to a DB instance:

1. Stop any transactions from being written to the primary DB instance.
2. Wait for RDS Custom for Oracle to apply all updates to your Oracle replica.
3. Promote your Oracle replica by choosing the **Promote** option on the Amazon RDS console, the AWS CLI command `promote-read-replica`, or the `PromoteReadReplica` Amazon RDS API operation.

Promoting a Oracle replica takes a few minutes to complete. During the process, RDS Custom for Oracle stops replication and reboots your replica. When the reboot completes, the Oracle replica is available as a standalone DB instance.

Console

To promote an RDS Custom for Oracle replica to a standalone DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the Amazon RDS console, choose **Databases**.
The **Databases** pane appears. Each Oracle replica shows **Replica** in the **Role** column.
3. Choose the RDS Custom for Oracle replica that you want to promote.
4. For **Actions**, choose **Promote**.
5. On the **Promote Oracle replica** page, enter the backup retention period and the backup window for the newly promoted DB instance. You can't set this value to **0**.
6. When the settings are as you want them, choose **Promote Oracle replica**.

AWS CLI

To promote your RDS Custom for Oracle replica to a standalone DB instance, use the AWS CLI [promote-read-replica](#) command.

Example

For Linux, macOS, or Unix:

```
aws rds promote-read-replica \
--db-instance-identifier my-custom-read-replica \
--backup-retention-period 2 \
--preferred-backup-window 23:00-24:00
```

For Windows:

```
aws rds promote-read-replica ^
--db-instance-identifier my-custom-read-replica ^
--backup-retention-period 2 ^
--preferred-backup-window 23:00-24:00
```

RDS API

To promote your RDS Custom for Oracle replica to be a standalone DB instance, call the Amazon RDS API [PromoteReadReplica](#) operation with the required parameter **DBInstanceIdentifier**.

Backing up and restoring an Amazon RDS Custom for Oracle DB instance

Like Amazon RDS, RDS Custom creates and saves automated backups of your RDS Custom for Oracle DB instance during the backup window of your DB instance. You can also back up your DB instance manually.

The procedure is identical to taking a snapshot of an Amazon RDS DB instance. The first snapshot of an RDS Custom DB instance contains the data for the full DB instance. Subsequent snapshots are incremental.

Restore DB snapshots using either the AWS Management Console or the AWS CLI.

Topics

- [Creating an RDS Custom for Oracle snapshot \(p. 831\)](#)
- [Restoring from an RDS Custom for Oracle DB snapshot \(p. 832\)](#)
- [Restoring an RDS Custom for Oracle instance to a point in time \(p. 833\)](#)
- [Deleting an RDS Custom for Oracle snapshot \(p. 836\)](#)
- [Deleting RDS Custom for Oracle automated backups \(p. 836\)](#)

Creating an RDS Custom for Oracle snapshot

RDS Custom for Oracle creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. When your DB instance contains a container database (CDB), the snapshot of the instance includes the root CDB and all PDBs.

When you create an RDS Custom for Oracle snapshot, specify which RDS Custom DB instance to back up. Give your snapshot a name so you can restore from it later.

When you create a snapshot, RDS Custom for Oracle creates an Amazon EBS snapshot for every volume attached to the DB instance. RDS Custom for Oracle uses the EBS snapshot of the root volume to register a new Amazon Machine Image (AMI). To make snapshots easy to associate with a specific DB instance, they're tagged with `DBSnapshotIdentifier`, `DbiResourceId`, and `VolumeType`.

Creating a DB snapshot results in a brief I/O suspension. This suspension can last from a few seconds to a few minutes, depending on the size and class of your DB instance. The snapshot creation time varies with the size of your database. Because the snapshot includes the entire storage volume, the size of files, such as temporary files, also affects snapshot creation time. To learn more about creating snapshots, see [Creating a DB snapshot \(p. 448\)](#).

Create an RDS Custom for Oracle snapshot using the console or the AWS CLI.

Console

To create an RDS Custom snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. In the list of RDS Custom DB instances, choose the instance for which you want to take a snapshot.
4. For **Actions**, choose **Take snapshot**.

The **Take DB snapshot** window appears.

5. For **Snapshot name**, enter the name of the snapshot.

6. Choose **Take snapshot**.

AWS CLI

You create a snapshot of an RDS Custom DB instance by using the [create-db-snapshot](#) AWS CLI command.

Specify the following options:

- `--db-instance-identifier` – Identifies which RDS Custom DB instance you are going to back up
- `--db-snapshot-identifier` – Names your RDS Custom snapshot so you can restore from it later

In this example, you create a DB snapshot called *my-custom-snapshot* for an RDS Custom DB instance called *my-custom-instance*.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-snapshot \
  --db-instance-identifier my-custom-instance \
  --db-snapshot-identifier my-custom-snapshot
```

For Windows:

```
aws rds create-db-snapshot ^
  --db-instance-identifier my-custom-instance ^
  --db-snapshot-identifier my-custom-snapshot
```

Restoring from an RDS Custom for Oracle DB snapshot

When you restore an RDS Custom for Oracle DB instance, you provide the name of the DB snapshot and a name for the new instance. You can't restore from a snapshot to an existing RDS Custom DB instance. A new RDS Custom for Oracle DB instance is created when you restore.

The restore process differs in the following ways from restore in Amazon RDS:

- Before restoring a snapshot, RDS Custom for Oracle backs up existing configuration files. These files are available on the restored instance in the directory `/rdsbdbdata/config/backup`. RDS Custom for Oracle restores the DB snapshot with default parameters and overwrites the previous database configuration files with existing ones. Thus, the restored instance doesn't preserve custom parameters and changes to database configuration files.
- The restored database has the same name as in the snapshot. You can't specify a different name. (For RDS Custom for Oracle, the default is ORCL.)

Console

To restore an RDS Custom DB instance from a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to restore from.

4. For **Actions**, choose **Restore snapshot**.
5. On the **Restore DB instance** page, for **DB instance identifier**, enter the name for your restored RDS Custom DB instance.
6. Choose **Restore DB instance**.

AWS CLI

You restore an RDS Custom DB snapshot by using the [restore-db-instance-from-db-snapshot](#) AWS CLI command.

If the snapshot you are restoring from is for a private DB instance, make sure to specify both the correct db-subnet-group-name and no-publicly-accessible. Otherwise, the DB instance defaults to publicly accessible. The following options are required:

- **db-snapshot-identifier** – Identifies the snapshot from which to restore
- **db-instance-identifier** – Specifies the name of the RDS Custom DB instance to create from the DB snapshot
- **custom-iam-instance-profile** – Specifies the instance profile associated with the underlying Amazon EC2 instance of an RDS Custom DB instance.

The following code restores the snapshot named `my-custom-snapshot` for `my-custom-instance`.

Example

For Linux, macOS, or Unix:

```
aws restore-db-instance-from-db-snapshot \
--db-snapshot-identifier my-custom-snapshot \
--db-instance-identifier my-custom-instance \
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
--no-publicly-accessible
```

For Windows:

```
aws restore-db-instance-from-db-snapshot ^
--db-snapshot-identifier my-custom-snapshot ^
--db-instance-identifier my-custom-instance ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
--no-publicly-accessible
```

Restoring an RDS Custom for Oracle instance to a point in time

You can restore a DB instance to a specific point in time (PITR), creating a new DB instance. To support PITR, your DB instances must have backup retention set to a nonzero value.

The latest restorable time for an RDS Custom for Oracle DB instance depends on several factors, but is typically within 5 minutes of the current time. To see the latest restorable time for a DB instance, use the AWS CLI [describe-db-instances](#) command and look at the value returned in the LatestRestorableTime field for the DB instance. To see the latest restorable time for each DB instance in the Amazon RDS console, choose **Automated backups**.

You can restore to any point in time within your backup retention period. To see the earliest restorable time for each DB instance, choose **Automated backups** in the Amazon RDS console.

For general information about PITR, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Topics

- [PITR considerations for RDS Custom for Oracle \(p. 834\)](#)

PITR considerations for RDS Custom for Oracle

In RDS Custom for Oracle, PITR differs in the following important ways from PITR in Amazon RDS:

- The restored database has the same name as in the source DB instance. You can't specify a different name. The default is ORCL.
- AWSRDSCustomIamRolePolicy requires new permissions. For more information, see [Add an access policy to AWSRDSCustomInstanceRoleForRdsCustomInstance \(p. 771\)](#).
- All RDS Custom for Oracle DB instances must have backup retention set to a nonzero value.
- If you change the operating system or DB instance time zone, PITR might not work. For information about changing time zones, see [Changing the time zone of an RDS Custom for Oracle DB instance \(p. 822\)](#).
- If you set automation to ALL_PAUSED, RDS Custom pauses the upload of archived redo logs, including logs created before the latest restorable time (LRT). We recommend that you pause automation for a brief period.

To illustrate, assume that your LRT is 10 minutes ago. You pause automation. During the pause, RDS Custom doesn't upload archived redo logs. If your DB instance crashes, you can only recover to a time before the LRT that existed when you paused. When you resume automation, RDS Custom resumes uploading logs. The LRT advances. Normal PITR rules apply.

- In RDS Custom, you can manually specify an arbitrary number of hours to retain archived redo logs before RDS Custom deletes them after upload. In RDS Custom, specify the number of hours manually in the following file: /opt/aws/rdscustomagent/config/redo_logs_custom_configuration.json. The format is {"archivedLogRetentionHours" : "*num_of_hours*"}. The number must be an integer in the range 1–840.
- Assume that you plug a non-CDB into a container database (CDB) as a PDB and then attempt PITR. The operation succeeds only if you previously backed up the PDB. After you create or modify a PDB, we recommend that you always back it up.
- We recommend that you don't customize database initialization parameters. For example, modifying the following parameters affects PITR:
 - CONTROL_FILE_RECORD_KEEP_TIME affects the rules for uploading and deleting logs.
 - LOG_ARCHIVE_DEST_n doesn't support multiple destinations.
 - ARCHIVE_LAG_TARGET affects the latest restorable time.
- If you customize database initialization parameters, we strongly recommend that you only customize the following:
 - COMPATIBLE
 - MAX_STRING_SIZE
 - DB_FILES
 - UNDO_TABLESPACE
 - ENABLE_PLUGGABLE_DATABASE
 - CONTROL_FILES
 - AUDIT_TRAIL
 - AUDIT_TRAIL_DEST

For all other initialization parameters, RDS Custom restores the default values. If you modify a parameter that isn't in the preceding list, it might have an adverse effect on PITR and lead to unpredictable results. For example, CONTROL_FILE_RECORD_KEEP_TIME affects the rules for uploading and deleting logs.

You can restore an RDS Custom DB instance to a point in time using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore an RDS Custom DB instance to a specified time

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Automated backups**.
3. Choose the RDS Custom DB instance that you want to restore.
4. For **Actions**, choose **Restore to point in time**.
The **Restore to point in time** window appears.
5. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time to which you want to restore the instance.

Times are shown in your local time zone, which is indicated by an offset from Coordinated Universal Time (UTC). For example, UTC-5 is Eastern Standard Time/Central Daylight Time.

6. For **DB instance identifier**, enter the name of the target restored RDS Custom DB instance. The name must be unique.
7. Choose other options as needed, such as DB instance class.
8. Choose **Restore to point in time**.

AWS CLI

You restore a DB instance to a specified time by using the [restore-db-instance-to-point-in-time](#) AWS CLI command to create a new RDS Custom DB instance.

Use one of the following options to specify the backup to restore from:

- `--source-db-instance-identifier mysourcedbinstance`
- `--source-dbi-resource-id dbinstanceresourceID`
- `--source-db-instance-automated-backups-arn backupARN`

The `custom-iam-instance-profile` option is required.

The following example restores `my-custom-db-instance` to a new DB instance named `my-restored-custom-db-instance`, as of the specified time.

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-identifier my-custom-db-instance \
    --target-db-instance-identifier my-restored-custom-db-instance \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
    --restore-time 2022-10-14T23:45:00.000Z
```

For Windows:

```
aws rds restore-db-instance-to-point-in-time ^
--source-db-instance-identifier my-custom-db-instance ^
--target-db-instance-identifier my-restored-custom-db-instance ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
--restore-time 2022-10-14T23:45:00.000Z
```

Deleting an RDS Custom for Oracle snapshot

You can delete DB snapshots managed by RDS Custom for Oracle when you no longer need them. The deletion procedure is the same for both Amazon RDS and RDS Custom DB instances.

The Amazon EBS snapshots for the binary and root volumes remain in your account for a longer time because they might be linked to some instances running in your account or to other RDS Custom for Oracle snapshots. These EBS snapshots are automatically deleted after they're no longer related to any existing RDS Custom for Oracle resources (DB instances or backups).

Console

To delete a snapshot of an RDS Custom DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to delete.
4. For **Actions**, choose **Delete snapshot**.
5. Choose **Delete** on the confirmation page.

AWS CLI

To delete an RDS Custom snapshot, use the AWS CLI command `delete-db-snapshot`.

The following option is required:

- `--db-snapshot-identifier` – The snapshot to be deleted

The following example deletes the `my-custom-snapshot` DB snapshot.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-snapshot \
--db-snapshot-identifier my-custom-snapshot
```

For Windows:

```
aws rds delete-db-snapshot ^
--db-snapshot-identifier my-custom-snapshot
```

Deleting RDS Custom for Oracle automated backups

You can delete retained automated backups for RDS Custom for Oracle when they are no longer needed. The procedure is the same as the procedure for deleting Amazon RDS backups.

Console

To delete a retained automated backup

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Automated backups**.
3. Choose **Retained**.
4. Choose the retained automated backup that you want to delete.
5. For **Actions**, choose **Delete**.
6. On the confirmation page, enter **delete me** and choose **Delete**.

AWS CLI

You can delete a retained automated backup by using the AWS CLI command [delete-db-instance-automated-backup](#).

The following option is used to delete a retained automated backup:

- **--dbi-resource-id** – The resource identifier for the source RDS Custom DB instance.

You can find the resource identifier for the source DB instance of a retained automated backup by using the AWS CLI command [describe-db-instance-automated-backups](#).

The following example deletes the retained automated backup with source DB instance resource identifier `custom-db-123ABCEXAMPLE`.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-instance-automated-backup \
--dbi-resource-id custom-db-123ABCEXAMPLE
```

For Windows:

```
aws rds delete-db-instance-automated-backup ^
--dbi-resource-id custom-db-123ABCEXAMPLE
```

Upgrading a DB instance for Amazon RDS Custom for Oracle

You can upgrade an Amazon RDS Custom DB instance by modifying it to use a new custom engine version (CEV). For general information about upgrades, see [Upgrading a DB instance engine version \(p. 360\)](#).

Topics

- [Requirements and considerations for RDS Custom for Oracle upgrades \(p. 838\)](#)
- [Viewing valid upgrade targets for RDS Custom for Oracle DB instances \(p. 839\)](#)
- [Upgrading an RDS Custom DB instance \(p. 839\)](#)
- [Viewing pending upgrades for RDS Custom DB instances \(p. 840\)](#)
- [Troubleshooting an upgrade failure for an RDS Custom for Oracle DB instance \(p. 841\)](#)

Requirements and considerations for RDS Custom for Oracle upgrades

Before upgrading your DB instance, note the following requirements:

- You can upgrade your DB instance to a new CEV only if it already exists.
- You can upgrade your DB instance to a new CEV only if it uses the same installation parameter settings in the manifest. For example, you can't upgrade a database that uses the default Oracle home to a CEV that uses a nondefault Oracle home.
- You can upgrade your DB instance to a new minor version only. For example, you can't upgrade a DB instance using an Oracle Database 12c CEV to an Oracle Database 19c CEV.

Consider the following:

- We strongly recommend that you upgrade your RDS Custom for Oracle DB instance using CEVs. RDS Custom for Oracle automation synchronizes the patch metadata with the database binary on your DB instance.

In special circumstances, RDS Custom supports applying a "one-off" patch directly to the underlying Amazon EC2 instance directly using OPATCH. A valid use case might be a patch that you want to apply immediately, but the RDS Custom team is upgrading the CEV feature, causing a delay. To apply a patch manually, perform the following steps:

1. Pause RDS Custom automation.
2. Apply your patch to the database binaries on the Amazon EC2 instance.
3. Resume RDS Custom automation.

A disadvantage of the preceding technique is that you must apply the patch manually to every instance that you want to upgrade. In contrast, when you create a new CEV, you can create or upgrade multiple DB instances using the same CEV.

- When you upgrade your primary DB instance, RDS Custom for Oracle upgrades your read replicas automatically. You don't have to upgrade read replicas manually.
- When you upgrade a CEV, RDS Custom deletes the data in the bin volume of your DB instance.
- When you upgrade a container database (CDB), RDS Custom checks that all PDBs are open or could be opened. If these conditions aren't met, RDS Custom stops the check and returns the database to its original state without attempting the upgrade. If the conditions are met, RDS Custom patches the CDB root first, and then patches all other PDBs (including PDB\$SEED) in parallel.

After the patching process completes, RDS Custom attempts to open all PDBs. If any PDBs fail to open, you receive the following event: The following PDBs failed to open: *List-of-PDBs*. If RDS Custom fails to patch the CDB root or any PDBs, the instance is put into the PATCH_DB_FAILED state.

- You might want to perform a major version upgrade and a conversion of non-CDB to CDB at the same time. In this case, we recommend that you complete this goal in the following process:
 1. Create a new RDS Custom DB instance that uses the Oracle Multitenant architecture.
 2. Plug in a non-CDB into your CDB root, creating it as a PDB. Make sure that the non-CDB is the same major version as your CDB.
 3. Convert your PDB by running the `noncdb_to_pdb.sql` Oracle script.
 4. Validate your CDB instance.
 5. Upgrade your CDB instance.

Viewing valid upgrade targets for RDS Custom for Oracle DB instances

You can see existing CEVs on the **Custom engine versions** page in the AWS Management Console.

You can also use the `describe-db-engine-versions` AWS CLI command to find valid upgrades for your DB instances, as shown in the following example. This example assumes that a DB instance was created using the version 19.my_cev1, and that the upgrade versions 19.my_cev2 and 19.my_cev exist.

```
aws rds describe-db-engine-versions --engine custom-oracle-ee --engine-version 19.my_cev1
```

The output resembles the following.

```
{  
    "DBEngineVersions": [  
        {  
            "Engine": "custom-oracle-ee",  
            "EngineVersion": "19.my_cev1",  
            ...  
            "ValidUpgradeTarget": [  
                {  
                    "Engine": "custom-oracle-ee",  
                    "EngineVersion": "19.my_cev2",  
                    "Description": "19.my_cev2 description",  
                    "AutoUpgrade": false,  
                    "IsMajorVersionUpgrade": false  
                },  
                {  
                    "Engine": "custom-oracle-ee",  
                    "EngineVersion": "19.my_cev3",  
                    "Description": "19.my_cev3 description",  
                    "AutoUpgrade": false,  
                    "IsMajorVersionUpgrade": false  
                }  
            ]  
            ...  
        }  
    ]  
}
```

Upgrading an RDS Custom DB instance

To upgrade your RDS Custom DB instance, you modify it to use a new CEV.

Read replicas managed by RDS Custom are automatically upgraded after the primary DB instance is upgraded.

Console

To upgrade an RDS Custom DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **DB engine version**, choose the CEV to upgrade to, such as `19.my_cev3`.
5. Choose **Continue** to check the summary of modifications.
Choose **Apply immediately** to apply the changes immediately.
6. If your changes are correct, choose **Modify DB instance**. Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

AWS CLI

To upgrade an RDS Custom DB instance, use the `modify-db-instance` AWS CLI command with the following parameters:

- `--db-instance-identifier` – The DB instance to be upgraded
- `--engine-version` – The new CEV
- `--no-apply-immediately | --apply-immediately` – Whether to perform the upgrade immediately or wait until the scheduled maintenance window

The following example upgrades `my-custom-instance` to version `19.my_cev3`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --engine-version 19.my_cev3 \
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --engine-version 19.my_cev3 ^
  --apply-immediately
```

Viewing pending upgrades for RDS Custom DB instances

You can see pending upgrades for your Amazon RDS Custom DB instances by using the `describe-db-instances` or `describe-pending-maintenance-actions` AWS CLI command.

However, this approach doesn't work if you used the `--apply-immediately` option or if the upgrade is in progress.

The following `describe-db-instances` command shows pending upgrades for `my-custom-instance`.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

The output resembles the following.

```
{  
    "DBInstances": [  
        {  
            "DBInstanceIdentifier": "my-custom-instance",  
            "EngineVersion": "19.my_cev1",  
            ...  
            "PendingModifiedValues": {  
                "EngineVersion": "19.my_cev3"  
            }  
        }  
    ]  
}
```

The following shows use of the `describe-pending-maintenance-actions` command.

```
aws rds describe-pending-maintenance-actions
```

The output resembles the following.

```
{  
    "PendingMaintenanceActions": [  
        {  
            "ResourceIdentifier": "arn:aws:rds:us-west-2:123456789012:instance:my-custom-instance",  
            "PendingMaintenanceActionDetails": [  
                {  
                    "Action": "db-upgrade",  
                    "Description": "Upgrade to 19.my_cev3"  
                }  
            ]  
        }  
    ]  
}
```

Troubleshooting an upgrade failure for an RDS Custom for Oracle DB instance

If an RDS Custom DB instance upgrade fails, an RDS event is generated and the DB instance status becomes `upgrade-failed`.

You can see this status by using the `describe-db-instances` AWS CLI command, as shown in the following example.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

The output resembles the following.

```
{  
    "DBInstances": [  
        {  
            "DBInstanceIdentifier": "my-custom-instance",  
            "EngineVersion": "19.my_cev1",  
            ...  
        }  
    ]  
}
```

```
    ...
    "PendingModifiedValues": {
        "EngineVersion": "19.my_cev3"
    }
}
]
}
```

After an upgrade failure, all database actions are blocked except for modifying the DB instance to perform the following tasks:

- Retrying the same upgrade
- Pausing and resuming RDS Custom automation
- Point-in-time recovery (PITR)
- Deleting the DB instance

Note

If automation has been paused for the RDS Custom DB instance, you can't retry the upgrade until you resume automation.

The same actions apply to an upgrade failure for an RDS-managed read replica as for the primary.

For more information, see [Troubleshooting upgrades for RDS Custom for Oracle \(p. 899\)](#).

Working with RDS Custom for SQL Server

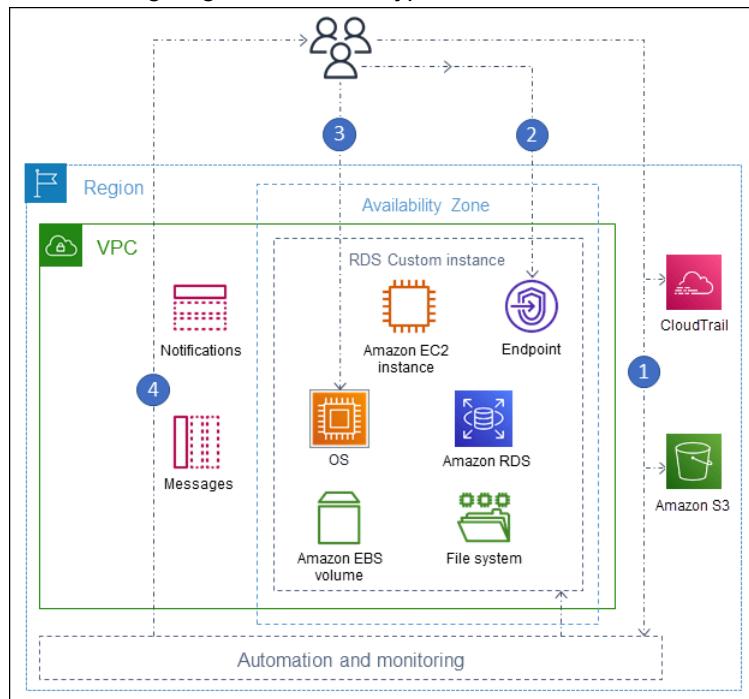
Following, you can find instructions for creating, managing, and maintaining your RDS Custom for SQL Server DB instances.

Topics

- [RDS Custom for SQL Server workflow \(p. 843\)](#)
- [Requirements and limitations for Amazon RDS Custom for SQL Server \(p. 845\)](#)
- [Setting up your environment for Amazon RDS Custom for SQL Server \(p. 847\)](#)
- [Creating and connecting to a DB instance for Amazon RDS Custom for SQL Server \(p. 860\)](#)
- [Managing an Amazon RDS Custom for SQL Server DB instance \(p. 868\)](#)
- [Backing up and restoring an Amazon RDS Custom for SQL Server DB instance \(p. 877\)](#)
- [Migrating an on-premises database to Amazon RDS Custom for SQL Server \(p. 885\)](#)
- [Upgrading a DB instance for Amazon RDS Custom for SQL Server \(p. 888\)](#)

RDS Custom for SQL Server workflow

The following diagram shows the typical workflow for RDS Custom for SQL Server.



The steps are as follows:

1. Create an RDS Custom for SQL Server DB instance from an engine version offered by RDS Custom.

For more information, see [Creating an RDS Custom for SQL Server DB instance \(p. 860\)](#).

2. Connect your application to the RDS Custom DB instance endpoint.

For more information, see [Connecting to your RDS Custom DB instance using AWS Systems Manager \(p. 863\)](#) and [Connecting to your RDS Custom DB instance using RDP \(p. 865\)](#).

3. (Optional) Access the host to customize your software.

4. Monitor notifications and messages generated by RDS Custom automation.

Creating a DB instance for RDS Custom

You create your RDS Custom DB instance using the `create-db-instance` command. The procedure is similar to creating an Amazon RDS instance. However, some of the parameters are different. For more information, see [Creating and connecting to a DB instance for Amazon RDS Custom for SQL Server \(p. 860\)](#).

Database connection

Like an Amazon RDS DB instance, your RDS Custom for SQL Server DB instance resides in a VPC. Your application connects to the RDS Custom instance using a client such as SQL Server Management Suite (SSMS), just as in RDS for SQL Server.

RDS Custom customization

You can access the RDS Custom host to install or customize software. To avoid conflicts between your changes and the RDS Custom automation, you can pause the automation for a specified period. During this period, RDS Custom doesn't perform monitoring or instance recovery. At the end of the period, RDS Custom resumes full automation. For more information, see [Pausing and resuming RDS Custom automation \(p. 868\)](#).

Requirements and limitations for Amazon RDS Custom for SQL Server

Following, you can find a summary of the Amazon RDS Custom for SQL Server requirements and limitations for quick reference. Requirements and limitations also appear in the relevant sections.

Topics

- [Region and version availability \(p. 845\)](#)
- [General requirements for RDS Custom for SQL Server \(p. 845\)](#)
- [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#)
- [Limitations for RDS Custom for SQL Server \(p. 846\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of Amazon RDS with Amazon RDS Custom for SQL Server, see [RDS Custom \(p. 110\)](#).

General requirements for RDS Custom for SQL Server

Make sure to follow these requirements for Amazon RDS Custom for SQL Server:

- Use the instance classes shown in [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#). The only storage types supported are solid state drives (SSD) of types gp2 and io1. The maximum storage limit is 16 TiB.
- Make sure that you have a symmetric encryption AWS KMS key to create an RDS Custom DB instance. For more information, see [Make sure that you have a symmetric encryption AWS KMS key \(p. 851\)](#).
- Make sure that you create an AWS Identity and Access Management (IAM) role and instance profile. For more information, see [Creating your IAM role and instance profile manually \(p. 852\)](#).
- Make sure to supply a networking configuration that RDS Custom can use to access other AWS services. For specific requirements, see [Configure networking, instance profile, and encryption \(p. 849\)](#).
- The combined number of RDS Custom and Amazon RDS DB instances can't exceed your quota limit. For example, if your quota is 40 DB instances, you can have 20 RDS Custom for SQL Server DB instances and 20 Amazon RDS DB instances.

DB instance class support for RDS Custom for SQL Server

RDS Custom for SQL Server supports the DB instance classes shown in the following table.

SQL Server edition	RDS Custom support
Enterprise Edition	db.r5.xlarge–db.r5.24xlarge db.m5.xlarge–db.m5.24xlarge
Standard Edition	db.r5.large–db.r5.24xlarge db.m5.large–db.m5.24xlarge

SQL Server edition	RDS Custom support
Web Edition	db.r5.large–db.r5.4xlarge db.m5.large–db.m5.4xlarge

Limitations for RDS Custom for SQL Server

The following limitations apply to RDS Custom for SQL Server:

- You can't provide your own custom DB engine version.
- You can't provide your own AMI.
- You can't create read replicas in Amazon RDS for RDS Custom for SQL Server DB instances. However, you can configure high availability manually using Always On Availability Groups. For more information, see [Working with high availability features for RDS Custom for SQL Server \(p. 868\)](#).
- You can't modify the time zone of an existing RDS Custom for SQL Server DB instance.
- You can't modify the server-level collation of an existing RDS Custom for SQL Server DB instance.
- Changes to the Microsoft Windows operating system or C: drive don't persist when you replace an Amazon EC2 instance. However, you can redo those changes using automation.
- Not all options are supported. For example, when you create an RDS Custom for SQL Server DB instance, you can't do the following:
 - Change the number of CPU cores and threads per core on the DB instance class.
 - Turn on storage autoscaling.
 - Create a Multi-AZ deployment. However, you can configure high availability manually using Always On Availability Groups. For more information, see [Working with high availability features for RDS Custom for SQL Server \(p. 868\)](#).
 - Configure Kerberos authentication using the AWS Management Console. However, you can configure Windows Authentication manually and use Kerberos.
 - Specify your own DB parameter group, option group, or character set.
 - Turn on Performance Insights.
 - Turn on automatic minor version upgrade.
- The maximum DB instance storage is 16 TiB.

Setting up your environment for Amazon RDS Custom for SQL Server

Before you create and manage a DB instance for Amazon RDS Custom for SQL Server DB instance, make sure to perform the following tasks.

Contents

- [Prerequisites for setting up RDS Custom for SQL Server \(p. 847\)](#)
- [Download and install the AWS CLI \(p. 848\)](#)
- [Grant required permissions to your IAM principal \(p. 848\)](#)
- [Configure networking, instance profile, and encryption \(p. 849\)](#)
 - [Configuring with AWS CloudFormation \(p. 849\)](#)
 - [Resources created by CloudFormation \(p. 849\)](#)
 - [Downloading the template file \(p. 850\)](#)
 - [Configuring resources using CloudFormation \(p. 850\)](#)
 - [Configuring manually \(p. 851\)](#)
 - [Make sure that you have a symmetric encryption AWS KMS key \(p. 851\)](#)
 - [Creating your IAM role and instance profile manually \(p. 852\)](#)
 - [Create the AWSRDSCustomSQLServerInstanceRole IAM role \(p. 852\)](#)
 - [Add an access policy to AWSRDSCustomSQLServerInstanceRole \(p. 852\)](#)
 - [Create your RDS Custom for SQL Server instance profile \(p. 856\)](#)
 - [Add AWSRDSCustomSQLServerInstanceRole to your RDS Custom for SQL Server instance profile \(p. 856\)](#)
 - [Configuring your VPC manually \(p. 856\)](#)
 - [Configure your VPC security group \(p. 857\)](#)
 - [Configure endpoints for dependent AWS services \(p. 857\)](#)
 - [Configure the instance metadata service \(p. 859\)](#)

Prerequisites for setting up RDS Custom for SQL Server

Before creating an RDS Custom for SQL Server DB instance, make sure that your environment meets the requirements described in this topic. Not all of them require action from you; if any action is necessary, the corresponding section describes it.

As part of this setup process, make sure to configure the specified AWS Identity and Access Management (IAM) users and roles. These are either used to create an RDS Custom DB instance or passed as a parameter in a creation request. If the account that you're using is part of an AWS organization, it might have service control policies (SCPs) restricting account level permissions. Make sure that the SCPs don't restrict the permissions on IAM users and roles that you create using the following procedures. For more information about SCPs, see [Service control policies \(SCPs\)](#) in the *AWS Organizations User Guide*. Use the [describe-organization](#) AWS CLI command to check whether your account is part of an AWS organization.

For each task, you can find descriptions following for the requirements and limitations specific to that task. For example, when you create your RDS Custom for SQL Server DB instance, use one of the SQL Server instances listed in [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#).

For general requirements that apply to RDS Custom for SQL Server, see [General requirements for RDS Custom for SQL Server \(p. 845\)](#).

Download and install the AWS CLI

You can use the AWS Command Line Interface (AWS CLI) to use RDS Custom features. You can use either version 1 or version 2 of the AWS CLI. For information about downloading and installing the AWS CLI, see [Installing or updating the latest version of the AWS CLI](#).

If you plan to access RDS Custom only from the AWS Management Console, skip this step.

If you have already downloaded the AWS CLI for Amazon RDS or RDS Custom for Oracle, skip this step.

Grant required permissions to your IAM principal

You use an IAM role or IAM user (referred to as the *IAM principal*) for creating an RDS Custom for SQL Server DB instance using the console or CLI. This IAM principal must have either of the following policies for successful DB instance creation:

- The `AdministratorAccess` policy
- The `AmazonRDSFullAccess` policy with the following additional permissions:

```
iam:SimulatePrincipalPolicy
cloudtrail>CreateTrail
cloudtrail:StartLogging
s3>CreateBucket
s3:PutBucketPolicy
s3:PutBucketObjectLockConfiguration
s3:PutBucketVersioning
kms>CreateGrant
kms:DescribeKey
```

For more information about the `kms:CreateGrant` permission, see [AWS KMS key management \(p. 2004\)](#).

The following sample JSON policy grants the required permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateIamRole",
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "*"
        },
        {
            "Sid": "CreateCloudTrail",
            "Effect": "Allow",
            "Action": [
                "cloudtrail>CreateTrail",
                "cloudtrail:StartLogging"
            ],
            "Resource": "arn:aws:cloudtrail:*::trail/do-not-delete-rds-custom-*"
        },
        {
            "Sid": "CreateS3Bucket",
            "Effect": "Allow",
            "Action": [
                "s3>CreateBucket",
                "s3:PutBucketPolicy",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ]
        }
    ]
}
```

```
        ],
        "Resource": "arn:aws:s3:::do-not-delete-rds-custom-*"
    },
    {
        "Sid": "CreateKmsGrant",
        "Effect": "Allow",
        "Action": [
            "kms:CreateGrant",
            "kms:DescribeKey"
        ],
        "Resource": "*"
    }
]
```

Also, the IAM principal requires the `iam:PassRole` permission on the IAM role. That must be attached to the instance profile passed in the `custom-iam-instance-profile` parameter in the request to create the RDS Custom DB instance. The instance profile and its attached role are created later in [Configure networking, instance profile, and encryption \(p. 849\)](#).

Make sure that the previously listed permissions aren't restricted by service control policies (SCPs), permission boundaries, or session policies associated with the IAM principal.

Configure networking, instance profile, and encryption

You can configure your IAM instance profile role, virtual private cloud (VPC), and AWS KMS symmetric encryption key by using either of the following processes:

- [Configuring with AWS CloudFormation \(p. 849\)](#) (recommended)
- [Configuring manually \(p. 851\)](#)

If your account is part of an AWS organization, make sure that the permissions required by the instance profile role aren't restricted by service control policies (SCPs).

The following networking configurations are designed to work best with DB instances that aren't publicly accessible. That is, you can't connect directly to the DB instance from outside the VPC.

Configuring with AWS CloudFormation

To simplify setup, you can use an AWS CloudFormation template file to create a CloudFormation stack. To learn how to create stacks, see [Creating a stack on the AWS CloudFormation console](#) in the *AWS CloudFormation User Guide*.

For a tutorial on how to launch Amazon RDS Custom for SQL Server using an AWS CloudFormation template, see [Get started with Amazon RDS Custom for SQL Server using an AWS CloudFormation template](#) in the *AWS Database Blog*.

Topics

- [Resources created by CloudFormation \(p. 849\)](#)
- [Downloading the template file \(p. 850\)](#)
- [Configuring resources using CloudFormation \(p. 850\)](#)

Resources created by CloudFormation

Successfully creating the CloudFormation stack creates the following resources in your AWS account:

- Symmetric encryption KMS key for encryption of data managed by RDS Custom.

- Instance profile and associated IAM role for attaching to RDS Custom instances.
- VPC with the CIDR range specified as the CloudFormation parameter. The default value is `10.0.0.0/16`.
- Two private subnets with the CIDR range specified in the parameters, and two different Availability Zones in the AWS Region. The default values for the subnet CIDRs are `10.0.128.0/20` and `10.0.144.0/20`.
- DHCP option set for the VPC with domain name resolution to an Amazon Domain Name System (DNS) server.
- Route table to associate with two private subnets and no access to the internet.
- Network access control list (ACL) to associate with two private subnets and access restricted to HTTPS.
- VPC security group to be associated with the RDS Custom instance. Access is restricted for outbound HTTPS to AWS service endpoints that are required by RDS Custom.
- VPC security group to be associated with VPC endpoints that are created for AWS service endpoints that are required by RDS Custom.
- DB subnet group in which RDS Custom instances are created.
- VPC endpoints for each of the AWS service endpoints that are required by RDS Custom.

Use the following procedures to create the CloudFormation stack for RDS Custom for SQL Server.

Downloading the template file

To download the template file

1. Open the context (right-click) menu for the link [custom-sqlserver-onboard.zip](#) and choose **Save Link As**.
2. Save the file to your computer.

Configuring resources using CloudFormation

To configure resources using CloudFormation

1. Open the CloudFormation console at <https://console.aws.amazon.com/cloudformation>.
2. To start the Create Stack wizard, choose **Create Stack**.

The **Create stack** page appears.

3. For **Prerequisite - Prepare template**, choose **Template is ready**.
4. For **Specify template**, do the following:
 - a. For **Template source**, choose **Upload a template file**.
 - b. For **Choose file**, navigate to and then choose `custom-sqlserver-onboard.json`.
5. Choose **Next**.

The **Specify stack details** page appears.

6. For **Stack name**, enter `rds-custom-sqlserver`.
7. For **Parameters**, do the following:
 - a. To keep the default options, choose **Next**.
 - b. To change options, choose the appropriate CIDR block range for the VPC and two of its subnets, and then choose **Next**.

Read the description of each parameter carefully before changing parameters.

8. On the **Configure stack options** page, choose **Next**.
9. On the **Review rds-custom-sqlserver** page, do the following:
 - a. For **Capabilities**, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** check box.
 - b. Choose **Create stack**.

CloudFormation creates the resources that RDS Custom for SQL Server requires. If the stack creation fails, read through the **Events** tab to see which resource creation failed and its status reason.

The **Outputs** tab for this CloudFormation stack in the console should have information about all resources to be passed as parameters for creating an RDS Custom for SQL Server DB instance. Make sure to use the VPC security group and DB subnet group created by CloudFormation for RDS Custom DB instances. By default, RDS tries to attach the default VPC security group, which might not have the access that you need.

Note

When you delete a CloudFormation stack, all of the resources created by the stack are deleted except the KMS key. The KMS key goes into a pending-deletion state and is deleted after 30 days. To keep the KMS key, perform a [CancelKeyDeletion](#) operation during the 30-day grace period.

If you used CloudFormation to create resources, you can skip [Configuring manually \(p. 851\)](#).

Configuring manually

If you choose to configure resources manually, perform the following tasks.

Topics

- [Make sure that you have a symmetric encryption AWS KMS key \(p. 851\)](#)
- [Creating your IAM role and instance profile manually \(p. 852\)](#)
- [Configuring your VPC manually \(p. 856\)](#)

Make sure that you have a symmetric encryption AWS KMS key

A symmetric encryption AWS KMS key is required for RDS Custom. When you create an RDS Custom for SQL Server DB instance, make sure to supply the KMS key identifier. For more information, see [Creating and connecting to a DB instance for Amazon RDS Custom for SQL Server \(p. 860\)](#).

You have the following options:

- If you have an existing KMS key in your AWS account, you can use it with RDS Custom. No further action is necessary.
- If you already created a symmetric encryption KMS key for a different RDS Custom engine, you can reuse the same KMS key. No further action is necessary.
- If you don't have an existing symmetric encryption KMS key in your account, create a KMS key by following the instructions in [Creating keys](#) in the *AWS Key Management Service Developer Guide*.
- If you're creating a CEV or RDS Custom DB instance, and your KMS key is in a different AWS account, make sure to use the AWS CLI. You can't use the AWS console with cross-account KMS keys.

RDS Custom doesn't support AWS-managed KMS keys.

Make sure that the symmetric encryption key that you use gives the AWS Identity and Access Management (IAM) role in your IAM instance profile access to the `kms:Decrypt` and `kms:GenerateDataKey` operations. If you have a new symmetric encryption key in your account, no

changes are required. Otherwise, make sure that your symmetric encryption key's policy can give access to these operations.

[Creating your IAM role and instance profile manually](#)

To use RDS Custom for SQL Server, create an IAM instance profile and IAM role as described following.

To create the IAM instance profile and IAM roles for RDS Custom for SQL Server

1. Create the IAM role named AWSRDSCustomSQLServerInstanceRole with a trust policy that lets Amazon EC2 assume this role.
2. Add an access policy to AWSRDSCustomSQLServerInstanceRole.
3. Create an IAM instance profile for RDS Custom for SQL Server that is named AWSRDSCustomSQLServerInstanceProfile.
4. Add AWSRDSCustomSQLServerInstanceRole to the instance profile.

[Create the AWSRDSCustomSQLServerInstanceRole IAM role](#)

The following example creates the AWSRDSCustomSQLServerInstanceRole role. The trust policy lets Amazon EC2 assume the role.

```
aws iam create-role \
--role-name AWSRDSCustomSQLServerInstanceRole \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            }
        }
    ]
}'
```

[Add an access policy to AWSRDSCustomSQLServerInstanceRole](#)

When you embed an inline policy in a role, the inline policy is used as part of the role's access (permissions) policy. You create the AWSRDSCustomSQLServerIamRolePolicy policy, which lets Amazon EC2 get and receive messages and perform various actions.

Make sure that the permissions in the access policy aren't restricted by SCPs or permission boundaries associated with the instance profile role.

The following example creates the access policy named AWSRDSCustomSQLServerIamRolePolicy, and adds it to the AWSRDSCustomSQLServerInstanceRole role. This example assumes that the '\$REGION', '\$ACCOUNT_ID', and '\$CUSTOMER_KMS_KEY_ID' variables have been set. '\$CUSTOMER_KMS_KEY_ID' is the ID, not the Amazon Resource Name (ARN), of the KMS key that you defined in [Make sure that you have a symmetric encryption AWS KMS key \(p. 851\)](#).

```
aws iam put-role-policy \
--role-name AWSRDSCustomSQLServerInstanceRole \
--policy-name AWSRDSCustomSQLServerIamRolePolicy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ssmAgent1",
            "Effect": "Allow",
            "Action": "ssm:DescribeParameters",
            "Resource": "arn:aws:ssm:$REGION:$ACCOUNT_ID/parameters/*"
        }
    ]
}'
```

```

    "Effect": "Allow",
    "Action": [
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm>ListAssociations",
        "ssm:PutInventory",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateInstanceInformation",
        "ssm:GetManifest"
    ],
    "Resource": "*"
},
{
    "Sid": "ssmAgent2",
    "Effect": "Allow",
    "Action": [
        "ssm>ListInstanceAssociations",
        "ssm:PutComplianceItems",
        "ssm:UpdateAssociationStatus",
        "ssm:DescribeAssociation",
        "ssm:UpdateInstanceAssociationStatus"
    ],
    "Resource": "arn:aws:ec2:'$REGION':'$ACCOUNT_ID':instance/*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": "custom-sqlserver"
        }
    }
},
{
    "Sid": "ssmAgent3",
    "Effect": "Allow",
    "Action": [
        "ssm:UpdateAssociationStatus",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
    ],
    "Resource": "arn:aws:ssm:*:*:document/*"
},
{
    "Sid": "ssmAgent4",
    "Effect": "Allow",
    "Action": [
        "ssmmessages>CreateControlChannel",
        "ssmmessages>CreateDataChannel",
        "ssmmessages>OpenControlChannel",
        "ssmmessages>OpenDataChannel"
    ],
    "Resource": "*"
},
{
    "Sid": "ssmAgent5",
    "Effect": "Allow",
    "Action": [
        "ec2messages>AcknowledgeMessage",
        "ec2messages>DeleteMessage",
        "ec2messages>FailMessage",
        "ec2messages>GetEndpoint",
        "ec2messages>GetMessages",
        "ec2messages>SendReply"
    ],
    "Resource": "*"
},
{
    "Sid": "ssmAgent6",
    "Effect": "Allow",

```

```
"Action": [
    "ssm:GetParameters",
    "ssm:GetParameter"
],
"Resource": "arn:aws:ssm:*::parameter/*"
},
{
    "Sid": "ssmAgent7",
    "Effect": "Allow",
    "Action": [
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:DescribeAssociation"
    ],
    "Resource": "arn:aws:ssm:*::association/*"
},
{
    "Sid": "eccSnapshot1",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": [
        "arn:aws:ec2:'$REGION':'$ACCOUNT_ID':volume/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": "custom-sqlserver"
        }
    }
},
{
    "Sid": "eccSnapshot2",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshot",
    "Resource": [
        "arn:aws:ec2:'$REGION':snapshot/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": "custom-sqlserver"
        }
    }
},
{
    "Sid": "eccCreateTag",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": "custom-sqlserver",
            "ec2:CreateAction": [
                "CreateSnapshot"
            ]
        }
    }
},
{
    "Sid": "s3BucketAccess",
    "Effect": "Allow",
    "Action": [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload"
    ],
    "Resource": [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
    ]
}
```

```

        ],
    },
    {
        "Sid": "customerKMSEncryption",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey*"
        ],
        "Resource": [
            "arn:aws:kms:'$REGION':'$ACCOUNT_ID':key/'$CUSTOMER_KMS_KEY_ID'"
        ]
    },
    {
        "Sid": "readSecretsFromCP",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
        ],
        "Resource": [
            "arn:aws:secretsmanager:'$REGION':'$ACCOUNT_ID':secret:do-not-delete-
rds-custom-*"
        ],
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSRDSCustom": "custom-sqlserver"
            }
        }
    },
    {
        "Sid": "publishCWMetrics",
        "Effect": "Allow",
        "Action": "cloudwatch:PutMetricData",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "cloudwatch:namespace": "rdscustom/rds-custom-sqlserver-agent"
            }
        }
    },
    {
        "Sid": "putEventsToEventBus",
        "Effect": "Allow",
        "Action": "events:PutEvents",
        "Resource": "arn:aws:events:'$REGION':'$ACCOUNT_ID':event-bus/default"
    },
    {
        "Sid": "cwlOperations1",
        "Effect": "Allow",
        "Action": [
            "logs:PutRetentionPolicy",
            "logs:PutLogEvents",
            "logs:DescribeLogStreams",
            "logs>CreateLogStream",
            "logs>CreateLogGroup"
        ],
        "Resource": "arn:aws:logs:'$REGION':'$ACCOUNT_ID':log-group:rds-custom-
instance-*"
    },
    {
        "Sid": "cwlOperations2",
        "Effect": "Allow",
        "Action": "logs:DescribeLogGroups",
        "Resource": "arn:aws:logs:'$REGION':'$ACCOUNT_ID':log-group:*

```

```
    ]'  
}'
```

Create your RDS Custom for SQL Server instance profile

Create your instance profile as follows, naming it `AWSRDSCustomSQLServerInstanceProfile`.

```
aws iam create-instance-profile \  
  --instance-profile-name AWSRDSCustomSQLServerInstanceProfile
```

Add `AWSRDSCustomSQLServerInstanceRole` to your RDS Custom for SQL Server instance profile

Add the `AWSRDSCustomInstanceRoleForRdsCustomInstance` role to the `AWSRDSCustomSQLServerInstanceProfile` profile.

```
aws iam add-role-to-instance-profile \  
  --instance-profile-name AWSRDSCustomSQLServerInstanceProfile \  
  --role-name AWSRDSCustomSQLServerInstanceRole
```

Configuring your VPC manually

Your RDS Custom DB instance is in a virtual private cloud (VPC) based on the Amazon VPC service, just like an Amazon EC2 instance or Amazon RDS instance. You provide and configure your own VPC. Thus, you have full control over your instance networking setup.

RDS Custom sends communication from your DB instance to other AWS services. To make sure that RDS Custom can communicate, it validates network connectivity to these services.

Your DB instance communicates with the following AWS services:

- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CloudWatch Events
- Amazon EC2
- Amazon EventBridge
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Make sure that VPC components involved in communication between the DB instance and AWS services are configured with the following requirements:

- The DB instance can make outbound connections on port 443 to other AWS services.
- The VPC allows incoming responses to requests originating from your DB instance.
- Correctly resolve the domain names of endpoints for each AWS service.

If you already configured a VPC for a different RDS Custom engine, you can reuse that VPC and skip this process.

Topics

- [Configure your VPC security group \(p. 857\)](#)
- [Configure endpoints for dependent AWS services \(p. 857\)](#)
- [Configure the instance metadata service \(p. 859\)](#)

Configure your VPC security group

A *security group* acts as a virtual firewall for a VPC instance, controlling both inbound and outbound traffic. An RDS Custom DB instance has a default security group that protects the instance. Make sure that your security group permits traffic between RDS Custom and other AWS services.

To configure your security group for RDS Custom

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc>.
2. Allow RDS Custom to use the default security group, or create your own security group.

For detailed instructions, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

3. Make sure that your security group permits outbound connections on port 443. RDS Custom needs this port to communicate with dependent AWS services.
4. If you have a private VPC and use VPC endpoints, make sure that the security group associated with the DB instance allows outbound connections on port 443 to VPC endpoints. Also make sure that the security group associated with the VPC endpoint allows inbound connections on port 443 from the DB instance.

If incoming connections aren't allowed, the RDS Custom instance can't connect to the AWS Systems Manager and Amazon EC2 endpoints. For more information, see [Create a Virtual Private Cloud endpoint](#) in the *AWS Systems Manager User Guide*.

For more information about security groups, see [Security groups for your VPC](#) in the *Amazon VPC Developer Guide*.

Configure endpoints for dependent AWS services

Make sure that your VPC allows outbound traffic to the following AWS services with which the DB instance communicates:

- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon CloudWatch Events
- Amazon EC2
- Amazon EventBridge
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

We recommend that you add endpoints for every service to your VPC using the following instructions. However, you can use any solution that lets your VPC communicate with AWS service endpoints. For example, you can use Network Address Translation (NAT) or AWS Direct Connect.

To configure endpoints for AWS services with which RDS Custom works

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. On the navigation bar, use the Region selector to choose the AWS Region.
3. In the navigation pane, choose **Endpoints**. In the main pane, choose **Create Endpoint**.
4. For **Service category**, choose **AWS services**.
5. For **Service Name**, choose the endpoint shown in the table.

6. For **VPC**, choose your VPC.
7. For **Subnets**, choose a subnet from each Availability Zone to include.

The VPC endpoint can span multiple Availability Zones. AWS creates an elastic network interface for the VPC endpoint in each subnet that you choose. Each network interface has a Domain Name System (DNS) host name and a private IP address.
8. For **Security group**, choose or create a security group.

You can use security groups to control access to your endpoint, much as you use a firewall. For more information about security groups, see [Security groups for your VPC](#) in the *Amazon VPC User Guide*.
9. Optionally, you can attach a policy to the VPC endpoint. Endpoint policies can control access to the AWS service to which you are connecting. The default policy allows all requests to pass through the endpoint. If you're using a custom policy, make sure that requests from the DB instance are allowed in the policy.
10. Choose **Create endpoint**.

The following table explains how to find the list of endpoints that your VPC needs for outbound communications.

Service	Endpoint format	Notes and links
AWS Systems Manager	Use the following endpoint formats: <ul style="list-style-type: none">• <code>ssm.region.amazonaws.com</code>• <code>ssmmessages.region.amazonaws.com</code>	For the list of endpoints in each Region, see AWS Systems Manager endpoints and quotas in the <i>Amazon Web Services General Reference</i> .
AWS Secrets Manager	Use the endpoint format <code>secretsmanager.region.amazonaws.com</code> .	For the list of endpoints in each Region, see AWS Secrets Manager endpoints and quotas in the <i>Amazon Web Services General Reference</i> .
Amazon CloudWatch	Use the following endpoint formats: <ul style="list-style-type: none">• For CloudWatch metrics, use <code>monitoring.region.amazonaws.com</code>• For CloudWatch Events, use <code>events.region.amazonaws.com</code>• For CloudWatch Logs, use <code>logs.region.amazonaws.com</code>	For the list of endpoints in every Region, see: <ul style="list-style-type: none">• Amazon CloudWatch endpoints and quotas in the Amazon Web Services General Reference• Amazon CloudWatch Logs endpoints and quotas in the Amazon Web Services General Reference• Amazon CloudWatch Events endpoints and quotas in the Amazon Web Services General Reference
Amazon EC2	Use the following endpoint formats: <ul style="list-style-type: none">• <code>ec2.region.amazonaws.com</code>• <code>ec2messages.region.amazonaws.com</code>	For the list of endpoints in each Region, see Amazon Elastic Compute Cloud endpoints and quotas in the <i>Amazon Web Services General Reference</i> .
Amazon S3	Use the endpoint format <code>s3.region.amazonaws.com</code> .	For the list of endpoints in each Region, see Amazon Simple Storage Service endpoints and quotas in the <i>Amazon Web Services General Reference</i> . To learn more about gateway endpoints for Amazon S3, see Endpoints for

Service	Endpoint format	Notes and links
		<p>Amazon S3 in the <i>Amazon VPC Developer Guide</i>.</p> <p>To learn how to create an access point, see Creating access points in the <i>Amazon VPC Developer Guide</i>.</p> <p>To learn how to create a gateway endpoints for Amazon S3, see Gateway VPC endpoints.</p>

Configure the instance metadata service

Make sure that your instance can do the following:

- Access the instance metadata service using Instance Metadata Service Version 2 (IMDSv2).
- Allow outbound communications through port 80 (HTTP) to the IMDS link IP address.
- Request instance metadata from `http://169.254.169.254`, the IMDSv2 link.

For more information, see [Use IMDSv2](#) in the *Amazon EC2 User Guide for Linux Instances*.

Creating and connecting to a DB instance for Amazon RDS Custom for SQL Server

You can create an RDS Custom DB instance, and then connect to it using AWS Systems Manager or Remote Desktop Protocol (RDP).

Important

Before you can create or connect to an RDS Custom for SQL Server DB instance, make sure to complete the tasks in [Setting up your environment for Amazon RDS Custom for SQL Server \(p. 847\)](#).

You can tag RDS Custom DB instances when you create them, but don't create or modify the AWSRDSCustom tag that's required for RDS Custom automation. For more information, see [Tagging RDS Custom for SQL Server resources \(p. 875\)](#).

The first time that you create an RDS Custom for SQL Server DB instance, you might receive the following error: The service-linked role is in the process of being created. Try again later. If you do, wait a few minutes and then try again to create the DB instance.

Topics

- [Creating an RDS Custom for SQL Server DB instance \(p. 860\)](#)
- [RDS Custom service-linked role \(p. 863\)](#)
- [Connecting to your RDS Custom DB instance using AWS Systems Manager \(p. 863\)](#)
- [Connecting to your RDS Custom DB instance using RDP \(p. 865\)](#)

Creating an RDS Custom for SQL Server DB instance

Create an Amazon RDS Custom for SQL Server DB instance using either the AWS Management Console or the AWS CLI. The procedure is similar to the procedure for creating an Amazon RDS DB instance.

For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Console

To create an RDS Custom for SQL Server DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose **Create database**.
4. Choose **Standard create** for the database creation method.
5. For **Engine options**, choose **Microsoft SQL Server** for the engine type.
6. For **Database management type**, choose **Amazon RDS Custom**.
7. In the **Edition** section, choose the DB engine edition that you want to use. For RDS Custom for SQL Server, the choices are Enterprise, Standard, and Web.
8. For **Database version**, keep the SQL Server 2019 default value.
9. For **Templates**, choose **Production**.
10. In the **Settings** section, enter a unique name for the **DB instance identifier**.
11. To enter your master password, do the following:
 - a. In the **Settings** section, open **Credential Settings**.
 - b. Clear the **Auto generate a password** check box.

- c. Change the **Master username** value and enter the same password in **Master password** and **Confirm password**.

By default, the new RDS Custom DB instance uses an automatically generated password for the master user.

12. In the **DB instance size** section, choose a value for **DB instance class**.

For supported classes, see [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#).

13. Choose **Storage** settings.

14. For **RDS Custom security**, do the following:

- a. For **IAM instance profile**, choose the instance profile for your RDS Custom for SQL Server DB instance.

The IAM instance profile must begin with AWSRDSCustom, for example *AWSRDSCustomInstanceProfileForRdsCustomInstance*.

- b. For **Encryption**, choose **Enter a key ARN** to list the available AWS KMS keys. Then choose your key from the list.

An AWS KMS key is required for RDS Custom. For more information, see [Make sure that you have a symmetric encryption AWS KMS key \(p. 851\)](#).

15. For the remaining sections, specify your preferred RDS Custom DB instance settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#). The following settings don't appear in the console and aren't supported:

- **Processor features**
- **Storage autoscaling**
- **Availability & durability**
- **Password and Kerberos authentication** option in **Database authentication** (only **Password authentication** is supported)
- **Database options** group in **Additional configuration**
- **Performance Insights**
- **Log exports**
- **Enable auto minor version upgrade**
- **Deletion protection**

Backup retention period is supported, but you can't choose **0 days**.

16. Choose **Create database**.

The **View credential details** button appears on the **Databases** page.

To view the master user name and password for the RDS Custom DB instance, choose **View credential details**.

To connect to the DB instance as the master user, use the user name and password that appear.

Important

You can't view the master user password again. If you don't record it, you might have to change it. To change the master user password after the RDS Custom DB instance is available, modify the DB instance. For more information about modifying a DB instance, see [Managing an Amazon RDS Custom for SQL Server DB instance \(p. 868\)](#).

17. Choose **Databases** to view the list of RDS Custom DB instances.

18. Choose the RDS Custom DB instance that you just created.

On the RDS console, the details for the new RDS Custom DB instance appear:

- The DB instance has a status of **creating** until the RDS Custom DB instance is created and ready for use. When the state changes to **available**, you can connect to the DB instance. Depending on the instance class and storage allocated, it can take several minutes for the new DB instance to be available.
- **Role** has the value **Instance (RDS Custom)**.
- **RDS Custom automation mode** has the value **Full automation**. This setting means that the DB instance provides automatic monitoring and instance recovery.

AWS CLI

You create an RDS Custom DB instance by using the [create-db-instance](#) AWS CLI command.

The following options are required:

- `--db-instance-identifier`
- `--db-instance-class` (for a list of supported instance classes, see [DB instance class support for RDS Custom for Oracle \(p. 766\)](#))
- `--engine` (`custom-sqlserver-ee`, `custom-sqlserver-se`, or `custom-sqlserver-web`)
- `--kms-key-id`
- `--custom-iam-instance-profile`

The following example creates an RDS Custom for SQL Server DB instance named `my-custom-instance`. The backup retention period is 3 days.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --engine custom-sqlserver-ee \
    --engine-version 15.00.4073.23.v1 \
    --db-instance-identifier my-custom-instance \
    --db-instance-class db.m5.xlarge \
    --allocated-storage 20 \
    --db-subnet-group mydbsubnetgroup \
    --master-username myuser \
    --master-user-password mypassword \
    --backup-retention-period 3 \
    --no-multi-az \
    --port 8200 \
    --license-model license-included \
    --kms-key-id mykmskey \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

For Windows:

```
aws rds create-db-instance ^
    --engine custom-sqlserver-ee ^
    --engine-version 15.00.4073.23.v1 ^
    --db-instance-identifier my-custom-instance ^
    --db-instance-class db.m5.xlarge ^
    --allocated-storage 20 ^
    --db-subnet-group mydbsubnetgroup ^
    --master-username myuser ^
```

```
--master-user-password mypassword ^
--backup-retention-period 3 ^
--no-multi-az ^
--port 8200 ^
--license-model license-included ^
--kms-key-id mykmskey ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

Get details about your instance by using the `describe-db-instances` command.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

The following partial output shows the engine, parameter groups, and other information.

```
{
    "DBInstances": [
        {
            "PendingModifiedValues": {},
            "Engine": "custom-sqlserver-ee",
            "MultiAZ": false,
            "DBSecurityGroups": [],
            "DBParameterGroups": [
                {
                    "DBParameterGroupName": "default.custom-sqlserver-ee-15",
                    "ParameterApplyStatus": "in-sync"
                }
            ],
            "AutomationMode": "full",
            "DBInstanceIdentifier": "my-custom-instance",
            "TagList": []
        }
    ]
}
```

RDS Custom service-linked role

A *service-linked role* gives Amazon RDS Custom access to resources in your AWS account. It makes using RDS Custom easier because you don't have to manually add the necessary permissions. RDS Custom defines the permissions of its service-linked roles, and unless defined otherwise, only RDS Custom can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy can't be attached to any other IAM entity.

When you create an RDS Custom DB instance, both the Amazon RDS and RDS Custom service-linked roles are created (if they don't already exist) and used. For more information, see [Using service-linked roles for Amazon RDS \(p. 2089\)](#).

The first time that you create an RDS Custom for SQL Server DB instance, you might receive the following error: The service-linked role is in the process of being created. Try again later. If you do, wait a few minutes and then try again to create the DB instance.

Connecting to your RDS Custom DB instance using AWS Systems Manager

After you create your RDS Custom DB instance, you can connect to it using AWS Systems Manager Session Manager. Session Manager is a Systems Manager capability that you can use to manage Amazon EC2 instances through a browser-based shell or through the AWS CLI. For more information, see [AWS Systems Manager Session Manager](#).

Console

To connect to your DB instance using Session Manager

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance to which you want to connect.
3. Choose **Configuration**.
4. Note the **Resource ID** value for your DB instance. For example, the resource ID might be db-ABCDEFHIJKLMNOPQRS0123456.
5. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
6. In the navigation pane, choose **Instances**.
7. Look for the name of your EC2 instance, and then choose the instance ID associated with it. For example, the instance ID might be i-abcdefhijklm01234.
8. Choose **Connect**.
9. Choose **Session Manager**.
10. Choose **Connect**.

A window opens for your session.

AWS CLI

You can connect to your RDS Custom DB instance using the AWS CLI. This technique requires the Session Manager plugin for the AWS CLI. To learn how to install the plugin, see [Install the Session Manager plugin for the AWS CLI](#).

To find the DB resource ID of your RDS Custom DB instance, use [describe-db-instances](#).

```
aws rds describe-db-instances \
--query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
--output text
```

The following sample output shows the resource ID for your RDS Custom instance. The prefix is db-.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

To find the EC2 instance ID of your DB instance, use `aws ec2 describe-instances`. The following example uses db-ABCDEFGHIJKLMNOPQRS0123456 for the resource ID.

```
aws ec2 describe-instances \
--filters "Name>tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
--output text \
--query 'Reservations[*].Instances[*].InstanceId'
```

The following sample output shows the EC2 instance ID.

```
i-abcdefhijklm01234
```

Use the `aws ssm start-session` command, supplying the EC2 instance ID in the `--target` parameter.

```
aws ssm start-session --target "i-abcdefhijklm01234"
```

A successful connection looks like the following.

```
Starting session with SessionId: yourid-abcdefghijklm1234
[ssm-user@ip-123-45-67-89 bin]$
```

Connecting to your RDS Custom DB instance using RDP

After you create your RDS Custom DB instance, you can connect to this instance using an RDP client. The procedure is the same as for connecting to an Amazon EC2 instance. For more information, see [Connect to your Windows instance](#).

To connect to the DB instance, you need the key pair associated with the instance. RDS Custom creates the key pair for you. The pair name uses the prefix do-not-delete-rds-custom-*DBInstanceIdentifier*. AWS Secrets Manager stores your private key as a secret.

Complete the task in the following steps:

1. [Configure your DB instance to allow RDP connections \(p. 865\)](#).
2. [Retrieve your secret key \(p. 866\)](#).
3. [Connect to your EC2 instance using the RDP utility \(p. 867\)](#).

Configure your DB instance to allow RDP connections

To allow RDP connections, configure your VPC security group and set a firewall rule on the host.

Configure your VPC security group

Make sure that the VPC security group associated with your DB instance permits inbound connections on port 3389 for Transmission Control Protocol (TCP). To learn how to configure your VPC security group, see [Configure your VPC security group \(p. 857\)](#).

Set the firewall rule on the host

To permit inbound connections on port 3389 for TCP, set a firewall rule on the host. The following examples show how to do this.

We recommend that you use the specific -Profile value: Public, Private, or Domain. Using Any refers to all three values. You can also specify a combination of values separated by a comma. For more information about setting firewall rules, see [Set-NetFirewallRule](#) in the Microsoft documentation.

To use Systems Manager Session Manager to set a firewall rule

1. Connect to Session Manager as shown in [Connecting to your RDS Custom DB instance using AWS Systems Manager \(p. 863\)](#).
2. Run the following command.

```
Set-NetFirewallRule -DisplayName "Remote Desktop - User Mode (TCP-In)" -Direction Inbound -LocalAddress Any -Profile Any
```

To use Systems Manager CLI commands to set a firewall rule

1. Use the following command to open RDP on the host.

```
OPEN_RDP_COMMAND_ID=$(aws ssm send-command --region $AWS_REGION \
--instance-ids $RDS_CUSTOM_INSTANCE_EC2_ID \
```

```
--document-name "AWS-RunPowerShellScript" \
--parameters '{"commands":["Set-NetFirewallRule -DisplayName \"Remote Desktop - User Mode (TCP-In)\" -Direction Inbound -LocalAddress Any -Profile Any"]}' \
--comment "Open RDP port" | jq -r ".Command.CommandId")
```

2. Use the command ID returned in the output to get the status of the previous command. To use the following query to return the command ID, make sure that you have the jq plug-in installed.

```
aws ssm list-commands \
--region $AWS_REGION \
--command-id $OPEN_RDP_COMMAND_ID
```

Retrieve your secret key

Retrieve your secret key using either AWS Management Console or the AWS CLI.

Console

To retrieve the secret key

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance to which you want to connect.
3. Choose the **Configuration** tab.
4. Note the **DB instance ID** for your DB instance, for example, *my-custom-instance*.
5. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
6. In the navigation pane, choose **Instances**.
7. Look for the name of your EC2 instance, and then choose the instance ID associated with it.
In this example, the instance ID is *i-abcdefgijklm01234*.
8. In **Details**, find **Key pair name**. The pair name includes the DB identifier. In this example, the pair name is *do-not-delete-rds-custom-my-custom-instance-0d726c*.
9. In the instance summary, find **Public IPv4 DNS**. For the example, the public DNS might be *ec2-12-345-678-901.us-east-2.compute.amazonaws.com*.
10. Open the AWS Secrets Manager console at <https://console.aws.amazon.com/secretsmanager/>.
11. Choose the secret that has the same name as your key pair.
12. Choose **Retrieve secret value**.

AWS CLI

To retrieve the private key

1. Get the list of your RDS Custom DB instances by calling the `aws rds describe-db-instances` command.

```
aws rds describe-db-instances \
--query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
--output text
```

2. Choose the DB instance identifier from the sample output, for example *do-not-delete-rds-custom-my-custom-instance*.
3. Find the EC2 instance ID of your DB instance by calling the `aws ec2 describe-instances` command. The following example uses the EC2 instance name to describe the DB instance.

```
aws ec2 describe-instances \
--filters "Name=tag:Name,Values=do-not-delete-rds-custom-my-custom-instance" \
--output text \
--query 'Reservations[*].Instances[*].InstanceId'
```

The following sample output shows the EC2 instance ID.

```
i-abcdefghijklm01234
```

4. Find the key name by specifying the EC2 instance ID, as shown in the following example.

```
aws ec2 describe-instances \
--instance-ids i-abcdefghijklm01234 \
--output text \
--query 'Reservations[*].Instances[*].KeyName'
```

The following sample output shows the key name, which uses the prefix do-not-delete-rds-custom-*DBInstanceIdentifier*.

```
do-not-delete-rds-custom-my-custom-instance-0d726c
```

Connect to your EC2 instance using the RDP utility

Follow the procedure in [Connect to your Windows instance using RDP](#) in the *Amazon EC2 User Guide for Windows Instances*. This procedure assumes that you created a .pem file that contains your private key.

Managing an Amazon RDS Custom for SQL Server DB instance

Amazon RDS Custom for SQL Server supports a subset of the usual management tasks for Amazon RDS DB instances. Following, you can find instructions for the supported RDS Custom for SQL Server management tasks using the AWS Management Console and the AWS CLI.

Topics

- [Working with high availability features for RDS Custom for SQL Server \(p. 868\)](#)
- [Pausing and resuming RDS Custom automation \(p. 868\)](#)
- [Modifying an RDS Custom for SQL Server DB instance \(p. 872\)](#)
- [Modifying the storage for an RDS Custom for SQL Server DB instance \(p. 873\)](#)
- [Support for Transparent Data Encryption \(p. 875\)](#)
- [Tagging RDS Custom for SQL Server resources \(p. 875\)](#)
- [Deleting an RDS Custom for SQL Server DB instance \(p. 875\)](#)

Working with high availability features for RDS Custom for SQL Server

To support replication between RDS Custom for SQL Server instances, you can configure high availability (HA) with Always On Availability Groups (AGs). The primary DB instance automatically synchronizes data to the standby instances.

You can configure your high availability environment in the following ways:

- Configure standby instances in different Availability Zones (AZs) to be resilient to AZ failures.
- Place your standby databases in mounted or read-only mode.
- Fail over or switch over from the primary database to a standby database with no data loss.
- Migrate data by configuring high availability for your on-premises instance, and then failing over or switching over to the RDS Custom standby database.

To learn how to configure high availability, see the blog post [Configure high availability with Always On Availability Groups on Amazon RDS Custom for SQL Server](#). You can perform the following tasks:

- Use a virtual private network (VPN) tunnel to encrypt data in transit for your high availability instances. Encryption in transit isn't configured automatically by RDS Custom.
- Configure Always On AGs to monitor your high availability instances.
- Allow the observer to perform automatic failover when necessary conditions are met.

You can also use other encryption technology, such as Secure Sockets Layer (SSL), to encrypt data in transit.

You're responsible for configuring VPC flow logs and CloudWatch alarms to monitor traffic mirroring to prevent data leakage.

Pausing and resuming RDS Custom automation

RDS Custom automatically provides monitoring and instance recovery for an RDS Custom for SQL Server DB instance. If you need to customize the instance, do the following:

1. Pause RDS Custom automation for a specified period. The pause ensures that your customizations don't interfere with RDS Custom automation.
2. Customize the RDS Custom for SQL Server DB instance as needed.
3. Do either of the following:
 - Resume automation manually.
 - Wait for the pause period to end. In this case, RDS Custom resumes monitoring and instance recovery automatically.

Important

Pausing and resuming automation are the only supported automation tasks when modifying an RDS Custom for SQL Server DB instance.

[Console](#)

To pause or resume RDS Custom automation

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **RDS Custom automation mode**, choose one of the following options:
 - **Paused** pauses the monitoring and instance recovery for the RDS Custom DB instance. Enter the pause duration that you want (in minutes) for **Automation mode duration**. The minimum value is 60 minutes (default). The maximum value is 1,440 minutes.
 - **Full automation** resumes automation.
5. Choose **Continue** to check the summary of modifications.

A message indicates that RDS Custom will apply the changes immediately.
6. If your changes are correct, choose **Modify DB instance**. Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

On the RDS console, the details for the modification appear. If you paused automation, the **Status** of your RDS Custom DB instance indicates **Automation paused**.
7. (Optional) In the navigation pane, choose **Databases**, and then your RDS Custom DB instance.

In the **Summary** pane, **RDS Custom automation mode** indicates the automation status. If automation is paused, the value is **Paused**. **Automation resumes in num minutes**.

[AWS CLI](#)

To pause or resume RDS Custom automation, use the [modify-db-instance](#) AWS CLI command. Identify the DB instance using the required parameter `--db-instance-identifier`. Control the automation mode with the following parameters:

- `--automation-mode` specifies the pause state of the DB instance. Valid values are `all-paused`, which pauses automation, and `full`, which resumes it.
- `--resume-full-automation-mode-minutes` specifies the duration of the pause. The default value is 60 minutes.

Note

Regardless of whether you specify `--no-apply-immediately` or `--apply-immediately`, RDS Custom applies modifications asynchronously as soon as possible.

In the command response, `ResumeFullAutomationModeTime` indicates the resume time as a UTC timestamp. When the automation mode is all-paused, you can use `modify-db-instance` to resume automation mode or extend the pause period. No other `modify-db-instance` options are supported.

The following example pauses automation for `my-custom-instance` for 90 minutes.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --automation-mode all-paused \
  --resume-full-automation-mode-minutes 90
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --automation-mode all-paused ^
  --resume-full-automation-mode-minutes 90
```

The following example extends the pause duration for an extra 30 minutes. The 30 minutes is added to the original time shown in `ResumeFullAutomationModeTime`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --automation-mode all-paused \
  --resume-full-automation-mode-minutes 30
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --automation-mode all-paused ^
  --resume-full-automation-mode-minutes 30
```

The following example resumes full automation for `my-custom-instance`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --automation-mode full \
```

For Windows:

```
aws rds modify-db-instance ^
```

```
--db-instance-identifier my-custom-instance ^
--automation-mode full
```

In the following partial sample output, the pending AutomationMode value is full.

```
{
    "DBInstance": {
        "PubliclyAccessible": true,
        "MasterUsername": "admin",
        "MonitoringInterval": 0,
        "LicenseModel": "bring-your-own-license",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "0123456789abcdefg"
            }
        ],
        "InstanceCreateTime": "2020-11-07T19:50:06.193Z",
        "CopyTagsToSnapshot": false,
        "OptionGroupMemberships": [
            {
                "Status": "in-sync",
                "OptionGroupName": "default:custom-oracle-ee-19"
            }
        ],
        "PendingModifiedValues": {
            "AutomationMode": "full"
        },
        "Engine": "custom-oracle-ee",
        "MultiAZ": false,
        "DBSecurityGroups": [],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.custom-oracle-ee-19",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        ...
        "ReadReplicaDBInstanceIdentifiers": [],
        "AllocatedStorage": 250,
        "DBInstanceArn": "arn:aws:rds:us-west-2:012345678912:db:my-custom-instance",
        "BackupRetentionPeriod": 3,
        "DBName": "ORCL",
        "PreferredMaintenanceWindow": "fri:10:56-fri:11:26",
        "Endpoint": {
            "HostedZoneId": "ABCDEFGHIJKLMNO",
            "Port": 8200,
            "Address": "my-custom-instance.abcdefghijklmno.us-west-2.rds.amazonaws.com"
        },
        "DBInstanceState": "automation-paused",
        "IAMDatabaseAuthenticationEnabled": false,
        "AutomationMode": "all-paused",
        "EngineVersion": "19.my_cev1",
        "DeletionProtection": false,
        "AvailabilityZone": "us-west-2a",
        "DomainMemberships": [],
        "StorageType": "gp2",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVWXYZ",
        "ResumeFullAutomationModeTime": "2020-11-07T20:56:50.565Z",
        "KmsKeyId": "arn:aws:kms:us-west-2:012345678912:key/
aa111a11-111a-11a1-1a11-1111a11a1a1a1",
        "StorageEncrypted": false,
        "AssociatedRoles": [],
        "DBInstanceClass": "db.m5.xlarge",
        "DbInstancePort": 0,
    }
}
```

```
    "DBInstanceIdentifier": "my-custom-instance",
    "TagList": []
}
```

Modifying an RDS Custom for SQL Server DB instance

Modifying an RDS Custom for SQL Server DB instance is similar to doing this for Amazon RDS, but the changes that you can make are limited to the following:

- Changing the DB instance class
- Changing the backup retention period and backup window
- Changing the maintenance window
- Upgrading the DB engine version when a new version becomes available

The following limitations apply to modifying an RDS Custom for SQL Server DB instance:

- Multi-AZ deployments aren't supported.
- Custom DB option and parameter groups aren't supported.
- Any storage volumes that you attach manually to your RDS Custom DB instance are outside the support perimeter.

For more information, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

Console

To modify an RDS Custom for SQL Server DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify.
4. Choose **Modify**.
5. Make the following changes as needed:
 - a. For **DB engine version**, choose the new version.
 - b. Change the value for **DB instance class**. For supported classes, see [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#)
 - c. Change the value for **Backup retention period**.
 - d. For **Backup window**, set values for the **Start time** and **Duration**.
 - e. For **DB instance maintenance window**, set values for the **Start day**, **Start time**, and **Duration**.
6. Choose **Continue**.
7. Choose **Apply immediately** or **Apply during the next scheduled maintenance window**.
8. Choose **Modify DB instance**.

AWS CLI

To modify an RDS Custom for SQL Server DB instance, use the `modify-db-instance` AWS CLI command. Set the following parameters as needed:

- `--db-instance-class` – For supported classes, see [DB instance class support for RDS Custom for SQL Server \(p. 845\)](#)

- `--engine-version` – The version number of the database engine to which you're upgrading.
- `--backup-retention-period` – How long to retain automated backups, from 0–35 days.
- `--preferred-backup-window` – The daily time range during which automated backups are created.
- `--preferred-maintenance-window` – The weekly time range (in UTC) during which system maintenance can occur.
- `--apply-immediately` – Use `--apply-immediately` to apply the storage changes immediately.
Or use `--no-apply-immediately` (the default) to apply the changes during the next maintenance window.

Modifying the storage for an RDS Custom for SQL Server DB instance

Modifying storage for an RDS Custom for SQL Server DB instance is similar to modifying storage for an Amazon RDS DB instance, but you can only do the following:

- Increase the allocated storage size.
- Change the storage type. For example, you can modify the storage type from io1 to gp2, or gp2 to io1.
- Change the provisioned IOPS, if you're using the volume types that supports provisioned IOPS, such as io1.

The following limitations apply to modifying the storage for an RDS Custom for SQL Server DB instance:

- The minimum allocated storage size for RDS Custom for SQL Server is 20 GiB, and the maximum supported storage size is 16 TiB.
- As with Amazon RDS, you can't decrease the allocated storage. This is a limitation of Amazon Elastic Block Store (Amazon EBS) volumes. For more information, see [Working with storage for Amazon RDS DB instances \(p. 410\)](#)
- Storage autoscaling isn't supported for RDS Custom for SQL Server DB instances.
- Any storage volumes that you manually attach to your RDS Custom DB instance are not considered for storage scaling. Only the RDS-provided default data volumes, i.e., the D drive, are considered for storage scaling.

For more information, see [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#).

- Scaling storage usually doesn't cause any outage or performance degradation of the DB instance. After you modify the storage size for a DB instance, the status of the DB instance is **storage-optimization**.
- Storage optimization can take several hours. You can't make further storage modifications for either six (6) hours or until storage optimization has completed on the instance, whichever is longer. For more information, see [Working with storage for Amazon RDS DB instances \(p. 410\)](#)

For more information about storage, see [Amazon RDS DB instance storage \(p. 64\)](#).

For general information about storage modification, see [Working with storage for Amazon RDS DB instances \(p. 410\)](#).

Console

To modify the storage for an RDS Custom for SQL Server DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify.
4. Choose **Modify**.
5. Make the following changes as needed:
 - a. Enter a new value for **Allocated storage**. It must be greater than the current value, and from 20 GiB–16 TiB.
 - b. Change the value for **Storage type**. You can use available storage types like General Purpose (gp2) or Provisioned IOPS (io1) storage.
 - c. If you are specifying volume types that support provisioned IOPS, you can define the **Provisioned IOPS** value.
6. Choose **Continue**.
7. Choose **Apply immediately** or **Apply during the next scheduled maintenance window**.
8. Choose **Modify DB instance**.

AWS CLI

To modify the storage for an RDS Custom for SQL Server DB instance, use the [modify-db-instance](#) AWS CLI command. Set the following parameters as needed:

- **--allocated-storage** – Amount of storage to be allocated for the DB instance, in gibibytes. It must be greater than the current value, and from 20–16,384 GiB.
- **--storage-type** – The storage type, for example, gp2 or io1.
- **--iops** – Provisioned IOPS for the DB instance. You can specify this only for storage types that support provisioned IOPS, like io1.
- **--apply-immediately** – Use **--apply-immediately** to apply the storage changes immediately.

Or use **--no-apply-immediately** (the default) to apply the changes during the next maintenance window.

The following example changes the storage size of my-custom-instance to 200 GiB, storage type to io1, and Provisioned IOPS to 3000.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier my-custom-instance \
  --storage-type io1 \
  --iops 3000 \
  --allocated-storage 200 \
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --storage-type io1 ^
  --iops 3000 ^
  --allocated-storage 200 ^
  --apply-immediately
```

Support for Transparent Data Encryption

RDS Custom supports Transparent Data Encryption (TDE) for RDS Custom for SQL Server DB instances.

However, you can't enable TDE using an option in a custom option group as you can in RDS for SQL Server. You turn on TDE manually. For information about Transparent Data Encryption for SQL Server, see [Transparent Data Encryption \(TDE\)](#) in the Microsoft documentation.

Tagging RDS Custom for SQL Server resources

You can tag RDS Custom resources as with Amazon RDS resources, but with some important differences:

- Don't create or modify the AWSRDSCustom tag that's required for RDS Custom automation. If you do, you might break the automation.
- Tags added to RDS Custom DB instances during creation are propagated to all other related RDS Custom resources.
- Tags aren't propagated when you add them to RDS Custom resources after DB instance creation.

For general information about resource tagging, see [Tagging Amazon RDS resources \(p. 392\)](#).

Deleting an RDS Custom for SQL Server DB instance

To delete an RDS Custom DB instance, do the following:

- Provide the name of the DB instance.
- Clear the option to take a final DB snapshot of the DB instance.
- Choose or clear the option to retain automated backups.

You can delete an RDS Custom DB instance using the console or the CLI. The time required to delete the DB instance can vary depending on the backup retention period (that is, how many backups to delete) and how much data is deleted.

Console

To delete an RDS Custom DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the RDS Custom DB instance that you want to delete. RDS Custom DB instances show the role **Instance (RDS Custom)**.
3. For **Actions**, choose **Delete**.
4. To retain automated backups, choose **Retain automated backups**.
5. Enter **delete me** in the box.
6. Choose **Delete**.

AWS CLI

You delete an RDS Custom DB instance by using the `delete-db-instance` AWS CLI command. Identify the DB instance using the required parameter `--db-instance-identifier`. The remaining parameters are the same as for an Amazon RDS DB instance, with the following exceptions:

- `--skip-final-snapshot` is required.
- `--no-skip-final-snapshot` isn't supported.

- `--final-db-snapshot-identifier` isn't supported.

The following example deletes the RDS Custom DB instance named `my-custom-instance`, and retains automated backups.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \
  --db-instance-identifier my-custom-instance \
  --skip-final-snapshot \
  --no-delete-automated-backups
```

For Windows:

```
aws rds delete-db-instance ^
  --db-instance-identifier my-custom-instance ^
  --skip-final-snapshot ^
  --no-delete-automated-backups
```

Backing up and restoring an Amazon RDS Custom for SQL Server DB instance

Like Amazon RDS, RDS Custom creates and saves automated backups of your RDS Custom for SQL Server DB instance during the backup window of your DB instance. You can also back up your DB instance manually.

The procedure is identical to taking a snapshot of an Amazon RDS DB instance. The first snapshot of an RDS Custom DB instance contains the data for the full DB instance. Subsequent snapshots are incremental.

Restore DB snapshots using either the AWS Management Console or the AWS CLI.

Topics

- [Creating an RDS Custom for SQL Server snapshot \(p. 877\)](#)
- [Restoring from an RDS Custom for SQL Server DB snapshot \(p. 878\)](#)
- [Restoring an RDS Custom for SQL Server instance to a point in time \(p. 879\)](#)
- [Deleting an RDS Custom for SQL Server snapshot \(p. 882\)](#)
- [Deleting RDS Custom for SQL Server automated backups \(p. 883\)](#)

Creating an RDS Custom for SQL Server snapshot

RDS Custom for SQL Server creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases. When you create a snapshot, specify which RDS Custom for SQL Server DB instance to back up. Give your snapshot a name so you can restore from it later.

When you create a snapshot, RDS Custom for SQL Server creates an Amazon EBS snapshot for every volume attached to the DB instance. RDS Custom for SQL Server uses the EBS snapshot of the root volume to register a new Amazon Machine Image (AMI). To make snapshots easy to associate with a specific DB instance, they're tagged with `DBSnapshotIdentifier`, `DBiResourceId`, and `VolumeType`.

Creating a DB snapshot results in a brief I/O suspension. This suspension can last from a few seconds to a few minutes, depending on the size and class of your DB instance. The snapshot creation time varies with the size of your database. Because the snapshot includes the entire storage volume, the size of files, such as temporary files, also affects snapshot creation time. To learn more about creating snapshots, see [Creating a DB snapshot \(p. 448\)](#).

Create an RDS Custom for SQL Server snapshot using the console or the AWS CLI.

Console

To create an RDS Custom snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. In the list of RDS Custom DB instances, choose the instance for which you want to take a snapshot.
4. For **Actions**, choose **Take snapshot**.

The **Take DB snapshot** window appears.

5. For **Snapshot name**, enter the name of the snapshot.
6. Choose **Take snapshot**.

AWS CLI

You create a snapshot of an RDS Custom DB instance by using the [create-db-snapshot](#) AWS CLI command.

Specify the following options:

- `--db-instance-identifier` – Identifies which RDS Custom DB instance you are going to back up
- `--db-snapshot-identifier` – Names your RDS Custom snapshot so you can restore from it later

In this example, you create a DB snapshot called *my-custom-snapshot* for an RDS Custom DB instance called *my-custom-instance*.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-snapshot \
  --db-instance-identifier my-custom-instance \
  --db-snapshot-identifier my-custom-snapshot
```

For Windows:

```
aws rds create-db-snapshot ^
  --db-instance-identifier my-custom-instance ^
  --db-snapshot-identifier my-custom-snapshot
```

Restoring from an RDS Custom for SQL Server DB snapshot

When you restore an RDS Custom for SQL Server DB instance, you provide the name of the DB snapshot and a name for the new instance. You can't restore from a snapshot to an existing RDS Custom DB instance. A new RDS Custom for SQL Server DB instance is created when you restore.

The restore process differs in the following ways from restore in Amazon RDS:

- Before restoring a snapshot, RDS Custom for SQL Server backs up existing configuration files. These files are available on the restored instance in the directory `/rdsdbdata/config/backup`. RDS Custom for SQL Server restores the DB snapshot with default parameters and overwrites the previous database configuration files with existing ones. Thus, the restored instance doesn't preserve custom parameters and changes to database configuration files.
- The restored database has the same name as in the snapshot. You can't specify a different name.

Console

To restore an RDS Custom DB instance from a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to restore from.
4. For **Actions**, choose **Restore snapshot**.
5. On the **Restore DB instance** page, for **DB instance identifier**, enter the name for your restored RDS Custom DB instance.

6. Choose Restore DB instance.

AWS CLI

You restore an RDS Custom DB snapshot by using the [restore-db-instance-from-db-snapshot](#) AWS CLI command.

If the snapshot you are restoring from is for a private DB instance, make sure to specify both the correct db-subnet-group-name and no-publicly-accessible. Otherwise, the DB instance defaults to publicly accessible. The following options are required:

- db-snapshot-identifier – Identifies the snapshot from which to restore
- db-instance-identifier – Specifies the name of the RDS Custom DB instance to create from the DB snapshot
- custom-iam-instance-profile – Specifies the instance profile associated with the underlying Amazon EC2 instance of an RDS Custom DB instance.

The following code restores the snapshot named my-custom-snapshot for my-custom-instance.

Example

For Linux, macOS, or Unix:

```
aws restore-db-instance-from-db-snapshot \
--db-snapshot-identifier my-custom-snapshot \
--db-instance-identifier my-custom-instance \
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
--no-publicly-accessible
```

For Windows:

```
aws restore-db-instance-from-db-snapshot ^
--db-snapshot-identifier my-custom-snapshot ^
--db-instance-identifier my-custom-instance ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
--no-publicly-accessible
```

Restoring an RDS Custom for SQL Server instance to a point in time

You can restore a DB instance to a specific point in time (PITR), creating a new DB instance. To support PITR, your DB instances must have backup retention set to a nonzero value.

The latest restorable time for an RDS Custom for SQL Server DB instance depends on several factors, but is typically within 5 minutes of the current time. To see the latest restorable time for a DB instance, use the AWS CLI [describe-db-instances](#) command and look at the value returned in the LatestRestorableTime field for the DB instance. To see the latest restorable time for each DB instance in the Amazon RDS console, choose **Automated backups**.

You can restore to any point in time within your backup retention period. To see the earliest restorable time for each DB instance, choose **Automated backups** in the Amazon RDS console.

For general information about PITR, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Topics

- [PITR considerations for RDS Custom for SQL Server \(p. 880\)](#)

PITR considerations for RDS Custom for SQL Server

In RDS Custom for SQL Server, PITR differs in the following important ways from PITR in Amazon RDS:

- PITR only restores the databases in the DB instance. It doesn't restore the operating system or files on the C: drive.
- For an RDS Custom for SQL Server DB instance, a database is backed up automatically and is eligible for PITR only under the following conditions:
 - The database is online.
 - Its recovery model is set to FULL.
 - It's writable.
 - It has its physical files on the D: drive.
 - It's not listed in the `rds_pitr_blocked_databases` table. For more information, see [Making databases ineligible for PITR \(p. 880\)](#).
- RDS Custom for SQL Server allows up to 5,000 databases per DB instance. However, the maximum number of databases restored by a PITR operation for an RDS Custom for SQL Server DB instance is 100. The 100 databases are determined by the order of their database ID.

Other databases that aren't part of PITR can be restored from DB snapshots, including the automated backups used for PITR.

- Adding a new database, renaming a database, or restoring a database that is eligible for PITR initiates a snapshot of the DB instance.
- Restored databases have the same name as in the source DB instance. You can't specify a different name.
- `AWSRDSCustomSQLServerIamRolePolicy` requires new permissions. For more information, see [Add an access policy to AWSRDSCustomSQLServerInstanceRole \(p. 852\)](#).
- Time zone changes aren't supported for RDS Custom for SQL Server. If you change the operating system or DB instance time zone, PITR (and other automation) doesn't work.

Making databases ineligible for PITR

You can specify that certain RDS Custom for SQL Server databases aren't part of automated backups and PITR. To do this, put their `database_id` values into a `rds_pitr_blocked_databases` table. Use the following SQL script to create the table.

To create the `rds_pitr_blocked_databases` table

- Run the following SQL script.

```
create table msdb..rds_pitr_blocked_databases
(
    database_id INT NOT NULL,
    database_name SYSNAME NOT NULL,
    db_entry_updated_date datetime NOT NULL DEFAULT GETDATE(),
    db_entry_updated_by SYSNAME NOT NULL DEFAULT CURRENT_USER,
    PRIMARY KEY (database_id)
);
```

For the list of eligible and ineligible databases, see the RI .End file in the RDSCustomForSQLServer/Instances/`DB_instance_resource_ID`/TransactionLogMetadata directory in the Amazon S3 bucket `do-not-delete-rds-custom-$ACCOUNT_ID-$REGION-unique_identifier`. For more information about the RI .End file, see [Transaction logs in Amazon S3 \(p. 881\)](#).

Transaction logs in Amazon S3

The backup retention period determines whether transaction logs for RDS Custom for SQL Server DB instances are automatically extracted and uploaded to Amazon S3. A nonzero value means that automatic backups are created, and that the RDS Custom agent uploads the transaction logs to S3 every 5 minutes.

Transaction log files on S3 are encrypted at rest using the AWS KMS key that you provided when you created your DB instance. For more information, see [Protecting data using server-side encryption](#) in the [Amazon Simple Storage Service User Guide](#).

The transaction logs for each database are uploaded to an S3 bucket named do-not-delete-rds-custom-\$ACCOUNT_ID-\$REGION-unique_identifier. The RDSCustomForSQLServer/Instances/DB_instance_resource_ID directory in the S3 bucket contains two subdirectories:

- TransactionLogs – Contains the transaction logs for each database and their respective metadata.

The transaction log file name follows the pattern *yyyyMMddHHmm.database_id.timestamp*, for example:

```
202110202230.11.1634769287
```

The same file name with the suffix _metadata contains information about the transaction log such as log sequence numbers, database name, and RdsChunkCount. RdsChunkCount determines how many physical files represent a single transaction log file. You might see files with suffixes _0001, _0002, and so on, which mean the physical chunks of a transaction log file. If you want to use a chunked transaction log file, make sure to merge the chunks after downloading them.

Consider a scenario where you have the following files:

- 202110202230.11.1634769287
- 202110202230.11.1634769287_0001
- 202110202230.11.1634769287_0002
- 202110202230.11.1634769287_metadata

The RdsChunkCount is 3. The order for merging the files is the following:

202110202230.11.1634769287, 202110202230.11.1634769287_0001,
202110202230.11.1634769287_0002.

- TransactionLogMetadata – Contains metadata information about each iteration of transaction log extraction.

The RI.End file contains information for all databases that had their transaction logs extracted, and all databases that exist but didn't have their transaction logs extracted. The RI.End file name follows the pattern *yyyyMMddHHmm.RI.End.timestamp*, for example:

```
202110202230.RI.End.1634769281
```

You can restore an RDS Custom for SQL Server DB instance to a point in time using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To restore an RDS Custom DB instance to a specified time

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Automated backups**.
3. Choose the RDS Custom DB instance that you want to restore.
4. For **Actions**, choose **Restore to point in time**.

The **Restore to point in time** window appears.

5. Choose **Latest restorable time** to restore to the latest possible time, or choose **Custom** to choose a time.

If you chose **Custom**, enter the date and time to which you want to restore the instance.

Times are shown in your local time zone, which is indicated by an offset from Coordinated Universal Time (UTC). For example, UTC-5 is Eastern Standard Time/Central Daylight Time.

6. For **DB instance identifier**, enter the name of the target restored RDS Custom DB instance. The name must be unique.
7. Choose other options as needed, such as DB instance class.
8. Choose **Restore to point in time**.

AWS CLI

You restore a DB instance to a specified time by using the [restore-db-instance-to-point-in-time](#) AWS CLI command to create a new RDS Custom DB instance.

Use one of the following options to specify the backup to restore from:

- `--source-db-instance-identifier mysourcedbinstance`
- `--source-db-instance-resource-id dbinstanceresourceID`
- `--source-db-instance-automated-backups-arn backupARN`

The `custom-iam-instance-profile` option is required.

The following example restores `my-custom-db-instance` to a new DB instance named `my-restored-custom-db-instance`, as of the specified time.

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-to-point-in-time \
  --source-db-instance-identifier my-custom-db-instance \
  --target-db-instance-identifier my-restored-custom-db-instance \
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
  --restore-time 2022-10-14T23:45:00.000Z
```

For Windows:

```
aws rds restore-db-instance-to-point-in-time ^
  --source-db-instance-identifier my-custom-db-instance ^
  --target-db-instance-identifier my-restored-custom-db-instance ^
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
  --restore-time 2022-10-14T23:45:00.000Z
```

Deleting an RDS Custom for SQL Server snapshot

You can delete DB snapshots managed by RDS Custom for SQL Server when you no longer need them. The deletion procedure is the same for both Amazon RDS and RDS Custom DB instances.

The Amazon EBS snapshots for the binary and root volumes remain in your account for a longer time because they might be linked to some instances running in your account or to other RDS Custom for SQL Server snapshots. These EBS snapshots are automatically deleted after they're no longer related to any existing RDS Custom for SQL Server resources (DB instances or backups).

Console

To delete a snapshot of an RDS Custom DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the DB snapshot that you want to delete.
4. For **Actions**, choose **Delete snapshot**.
5. Choose **Delete** on the confirmation page.

AWS CLI

To delete an RDS Custom snapshot, use the AWS CLI command `delete-db-snapshot`.

The following option is required:

- `--db-snapshot-identifier` – The snapshot to be deleted

The following example deletes the `my-custom-snapshot` DB snapshot.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-snapshot \
--db-snapshot-identifier my-custom-snapshot
```

For Windows:

```
aws rds delete-db-snapshot ^
--db-snapshot-identifier my-custom-snapshot
```

Deleting RDS Custom for SQL Server automated backups

You can delete retained automated backups for RDS Custom for SQL Server when they are no longer needed. The procedure is the same as the procedure for deleting Amazon RDS backups.

Console

To delete a retained automated backup

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Automated backups**.
3. Choose **Retained**.
4. Choose the retained automated backup that you want to delete.
5. For **Actions**, choose **Delete**.

6. On the confirmation page, enter **delete me** and choose **Delete**.

AWS CLI

You can delete a retained automated backup by using the AWS CLI command [delete-db-instance-automated-backup](#).

The following option is used to delete a retained automated backup:

- **--dbi-resource-id** – The resource identifier for the source RDS Custom DB instance.

You can find the resource identifier for the source DB instance of a retained automated backup by using the AWS CLI command [describe-db-instance-automated-backups](#).

The following example deletes the retained automated backup with source DB instance resource identifier `custom-db-123ABCEXAMPLE`.

Example

For Linux, macOS, or Unix:

```
aws rds delete-db-instance-automated-backup \
--dbi-resource-id custom-db-123ABCEXAMPLE
```

For Windows:

```
aws rds delete-db-instance-automated-backup ^
--dbi-resource-id custom-db-123ABCEXAMPLE
```

Migrating an on-premises database to Amazon RDS Custom for SQL Server

You can use the following process to migrate an on-premises Microsoft SQL Server database to Amazon RDS Custom for SQL Server using native backup and restore:

1. Take a full backup of the database on the on-premises DB instance.
2. Upload the backup file to Amazon S3.
3. Download the backup file from S3 to your RDS Custom for SQL Server DB instance.
4. Restore a database using the downloaded backup file on the RDS Custom for SQL Server DB instance.

This process explains the migration of a database from on-premises to RDS Custom for SQL Server, using native full backup and restore. To reduce the cutover time during the migration process, you might also consider using differential or log backups.

For general information about native backup and restore for RDS for SQL Server, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Topics

- [Prerequisites \(p. 885\)](#)
- [Backing up the on-premises database \(p. 885\)](#)
- [Uploading the backup file to Amazon S3 \(p. 886\)](#)
- [Downloading the backup file from Amazon S3 \(p. 886\)](#)
- [Restoring the backup file to the RDS Custom for SQL Server DB instance \(p. 886\)](#)

Prerequisites

Perform the following tasks before migrating the database:

1. Configure Remote Desktop Connection (RDP) for your RDS Custom for SQL Server DB instance. For more information, see [Connecting to your RDS Custom DB instance using RDP \(p. 865\)](#).
2. Configure access to Amazon S3 so you can upload and download the database backup file. For more information, see [Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 \(p. 1153\)](#).

Backing up the on-premises database

You use SQL Server native backup to take a full backup of the database on the on-premises DB instance.

The following example shows a backup of a database called `mydatabase`, with the `COMPRESSION` option specified to reduce the backup file size.

To back up the on-premises database

1. Using SQL Server Management Studio (SSMS), connect to the on-premises SQL Server instance.
2. Run the following T-SQL command.

```
backup database mydatabase to  
disk ='C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Backup\mydb-  
full-compressed.bak'  
with compression;
```

Uploading the backup file to Amazon S3

You use the AWS Management Console to upload the backup file `mydb-full-compressed.bak` to Amazon S3.

To upload the backup file to S3

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. For **Buckets**, choose the name of the bucket to which you want to upload your backup file.
3. Choose **Upload**.
4. In the **Upload** window, do one of the following:
 - Drag and drop `mydb-full-compressed.bak` to the **Upload** window.
 - Choose **Add file**, choose `mydb-full-compressed.bak`, and then choose **Open**.

Amazon S3 uploads your backup file as an S3 object. When the upload completes, you can see a success message on the **Upload: status** page.

Downloading the backup file from Amazon S3

You use the console to download the backup file from S3 to the RDS Custom for SQL Server DB instance.

To download the backup file from S3

1. Using RDP, connect to your RDS Custom for SQL Server DB instance.
2. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
3. In the **Buckets** list, choose the name of the bucket that contains your backup file.
4. Choose the backup file `mydb-full-compressed.bak`.
5. For **Actions**, choose **Download as**.
6. Open the context (right-click) menu for the link provided, then choose **Save As**.
7. Save `mydb-full-compressed.bak` to the `D:\rdsdbdata\BACKUP` directory.

Restoring the backup file to the RDS Custom for SQL Server DB instance

You use SQL Server native restore to restore the backup file to your RDS Custom for SQL Server DB instance.

In this example, the MOVE option is specified because the data and log file directories are different from the on-premises DB instance.

To restore the backup file

1. Using SSMS, connect to your RDS Custom for SQL Server DB instance.
2. Run the following T-SQL command.

```
restore database mydatabase from disk='D:\rdsdbdata\BACKUP\mydb-full-compressed.bak'  
with move 'mydatabase' to 'D:\rdsdbdata\DATA\mydatabase.mdf',  
move 'mydatabase_log' to 'D:\rdsdbdata\DATA\mydatabase_log.ldf';
```


Upgrading a DB instance for Amazon RDS Custom for SQL Server

You can upgrade an Amazon RDS Custom for SQL Server DB instance by modifying it to use a new DB engine version, the same as you do for Amazon RDS.

The same limitations for upgrading an RDS Custom for SQL Server DB instance apply as for modifying an RDS Custom for SQL Server DB instance in general. For more information, see [Modifying an RDS Custom for SQL Server DB instance \(p. 872\)](#).

For general information about upgrading DB instances, see [Upgrading a DB instance engine version \(p. 360\)](#).

Troubleshooting DB issues for Amazon RDS Custom

The shared responsibility model of RDS Custom provides OS shell-level access and database administrator access. RDS Custom runs resources in your account, unlike Amazon RDS, which runs resources in a system account. With greater access comes greater responsibility. In the following sections, you can learn how to troubleshoot issues with Amazon RDS Custom DB instances.

Topics

- [Viewing RDS Custom events \(p. 889\)](#)
- [Subscribing to event notifications \(p. 889\)](#)
- [Troubleshooting custom engine version creation for RDS Custom for Oracle \(p. 890\)](#)
- [RDS Custom support perimeter and unsupported configurations \(p. 891\)](#)
- [Fixing unsupported configurations \(p. 891\)](#)
- [How Amazon RDS Custom replaces an impaired host \(p. 897\)](#)
- [Troubleshooting upgrades for RDS Custom for Oracle \(p. 899\)](#)
- [Troubleshooting replica promotion for RDS Custom for Oracle \(p. 900\)](#)
- [Troubleshooting replica creation for RDS Custom for Oracle \(p. 900\)](#)

Viewing RDS Custom events

The procedure for viewing events is the same for RDS Custom and Amazon RDS DB instances. For more information, see [Viewing Amazon RDS events \(p. 647\)](#).

To view RDS Custom event notification using the AWS CLI, use the `describe-events` command. RDS Custom introduces several new events. The event categories are the same as for Amazon RDS. For the list of events, see [Amazon RDS event categories and event messages \(p. 668\)](#).

The following example retrieves details for the events that have occurred for the specified RDS Custom DB instance.

```
aws rds describe-events \
    --source-identifier my-custom-instance \
    --source-type db-instance
```

Subscribing to event notifications

The procedure for subscribing to events is the same for RDS Custom and Amazon RDS DB instances. For more information, see [Subscribing to Amazon RDS event notification \(p. 655\)](#).

To subscribe to RDS Custom event notification using the CLI, use `create-event-subscription` command. Include the following required parameters:

- `--subscription-name`
- `--sns-topic-arn`

The following example creates a subscription for backup and recovery events for an RDS Custom DB instance in the current AWS account. Notifications are sent to an Amazon Simple Notification Service (Amazon SNS) topic, specified by `--sns-topic-arn`.

```
aws rds create-event-subscription \
--subscription-name my-instance-events \
--source-type db-instance \
--event-categories '['backup","recovery"]' \
--sns-topic-arn arn:aws:sns:us-east-1:123456789012:interesting-events
```

Troubleshooting custom engine version creation for RDS Custom for Oracle

When CEV creation fails, RDS Custom issues RDS-EVENT-0198 with the message **Creation failed for custom engine version *major-engine-version.cev_name***, and includes details about the failure. For example, the event prints missing files.

CEV creation might fail because of the following issues:

- The Amazon S3 bucket containing your installation files isn't in the same AWS Region as your CEV.
- When you request CEV creation in an AWS Region for the first time, RDS Custom creates an S3 bucket for storing RDS Custom resources (such as CEV artifacts, AWS CloudTrail logs, and transaction logs).

CEV creation fails if RDS Custom can't create the S3 bucket. Either the caller doesn't have S3 permissions as described in [Grant required permissions to your IAM user \(p. 778\)](#), or the number of S3 buckets has reached the limit.

- The caller doesn't have permissions to get files from your S3 bucket that contains the installation media files. These permissions are described in [Adding necessary IAM permissions \(p. 798\)](#).
- Your IAM policy has an `aws:SourceIp` condition. Make sure to follow the recommendations in [AWS Denies access to AWS based on the source IP](#) in the *AWS Identity and Access Management User Guide*. Also make sure that the caller has the S3 permissions described in [Grant required permissions to your IAM user \(p. 778\)](#).
- Installation media files listed in the CEV manifest aren't in your S3 bucket.
- The SHA-256 checksums of the installation files are unknown to RDS Custom.

Confirm that the SHA-256 checksums of the provided files match the SHA-256 checksum on the Oracle website. If the checksums match, contact [AWS Support](#) and provide the failed CEV name, file name, and checksum.

- The OPatch version is incompatible with your patch files. You might get the following message: `OPatch is lower than minimum required version.` Check that the version meets the requirements for all patches, and try again. To apply an Oracle patch, you must use a compatible version of the OPatch utility. You can find the required version of the Opatch utility in the readme file for the patch. Download the most recent OPatch utility from My Oracle Support, and try creating your CEV again.
- The patches specified in the CEV manifest are in the wrong order.

You can view RDS events either on the RDS console (in the navigation pane, choose **Events**) or by using the `describe-events` AWS CLI command. The default duration is 60 minutes. If no events are returned, specify a longer duration, as shown in the following example.

```
aws rds describe-events --duration 360
```

Currently, the MediaImport service that imports files from Amazon S3 to create CEVs isn't integrated with AWS CloudTrail. Therefore, if you turn on data logging for Amazon RDS in CloudTrail, calls to the MediaImport service such as the `CreateCustomDbEngineVersion` event aren't logged.

However, you might see calls from the API gateway that accesses your Amazon S3 bucket. These calls come from the MediaImport service for the `CreateCustomDbEngineVersion` event.

RDS Custom support perimeter and unsupported configurations

RDS Custom provides monitoring capability called the *support perimeter*. The support perimeter ensures that your RDS Custom instance uses a supported AWS infrastructure, operating system, and database.

The support perimeter checks that the requirements listed in [Fixing unsupported configurations \(p. 891\)](#) are met. If any of these requirements aren't met, RDS Custom considers the DB instance to be outside of the support perimeter. RDS Custom then changes the DB instance status to unsupported-configuration, and sends event notifications. After you fix the configuration problems, RDS Custom changes the DB instance status to available.

What happens in the unsupported-configuration state

While the DB instance is in the unsupported-configuration state, the following is the case:

- You can't modify the DB instance.
- You can't take DB snapshots.
- Automated backups aren't created.
- RDS Custom automation doesn't replace the underlying Amazon EC2 instance if it becomes impaired.

However, the following RDS Custom automation continues to run:

- The RDS Custom agent monitors the DB instance and sends notifications to the support perimeter of further changes.
- The support perimeter continues to run and captures change events for the DB instance. This has two purposes:
 - When you fix the configuration that caused the DB instance to be in the unsupported-configuration state, the support perimeter can return the DB instance to the available state.
 - If you make other unsupported configurations, the support perimeter notifies you about them so that you can correct them.
- Redo logs are still archived and uploaded to Amazon S3 to facilitate point-in-time recovery (PITR). However, be aware of the following:
 - PITR can take a long time to completely restore to a new DB instance. This is because you can't take either automated or manual snapshots while the DB instance is in the unsupported-configuration state.

PITR has to replay more redo logs starting from the most recent snapshot taken before the instance entered the unsupported-configuration state.

- In some cases, the DB instance is in the unsupported-configuration state because of changes you made that impacted redo log upload functionality. In these cases, PITR can't restore the DB instance to the latest restorable time.

Fixing unsupported configurations

It's your responsibility to fix configuration issues that put your RDS Custom DB instance into the unsupported-configuration state. If the issue is with the AWS infrastructure, you can use the console or the AWS CLI to fix it. If the issue is with the operating system or the database configuration, you can log in to the host to fix it.

In the following table, you can find descriptions of the notifications that the support perimeter sends and how to fix them. These notifications and the support perimeter are subject to change.

Notification	Description	Action
Database health:	<ul style="list-style-type: none"> You need to manually recover the database on EC2 instance [i-XXXXXXXXXXXXXXXXXX]. The DB instance restarted. 	<p>The support perimeter monitors the DB instance state. It also monitors how many restarts occurred during the previous hour and day.</p> <p>You're notified when the instance is in a state where it still exists, but you can't interact with it.</p> <p>Log in to the host and examine the database state.</p> <pre>ps -eo pid,state,command grep smon</pre> <p>Restart the DB instance if necessary to get it running again. Sometimes it's necessary to reboot the host.</p> <p>After the restart, the RDS Custom agent detects that the DB instance is no longer in an unresponsive state. It then notifies the support perimeter to reevaluate the DB instance state.</p>
Database archive lag target (RDS Custom for Oracle only):	<ul style="list-style-type: none"> The monitored Archive Lag Target database parameter on Amazon EC2 instance [i-XXXXXXXXXXXXXXXXXX] has changed from [300] to [0]. The RDS Custom instance is using an unsupported configuration because of the following [1] issue(s): (1) The archive lag target database parameter on Amazon EC2 instance [i-XXXXXXXXXXXXXXXXXX] is out of desired range {"lowerbound":60,"upperbound":7200}. 	<p>The support perimeter monitors the ARCHIVE_LAG_TARGET database parameter to verify that the DB instance's latest restorable time is within reasonable bounds.</p> <p>Log in to the host, connect to the DB instance, and change the ARCHIVE_LAG_TARGET parameter to a value from 60–7200.</p> <p>For example, use the following SQL command.</p> <pre>alter system set archive_lag_target=300 scope=both;</pre> <p>The DB instance becomes available within 30 minutes.</p>
Database log mode (RDS Custom for Oracle only):	<p>The monitored log mode of the database on Amazon EC2 instance [i-XXXXXXXXXXXXXXXXXX] has changed from [ARCHIVELOG] to [NOARCHIVELOG].</p>	<p>The DB instance log mode must be set to ARCHIVELOG.</p> <p>Log in to the host and shut down the DB instance. You can use the following SQL command.</p> <pre>shutdown immediate;</pre> <p>The RDS Custom agent restarts the DB instance and sets the log mode to ARCHIVELOG.</p> <p>The DB instance becomes available within 30 minutes.</p>
RDS Custom agent status (RDS Custom for Oracle):	<p>The monitored state of the RDS Custom agent on EC2 instance</p>	<p>The RDS Custom agent must always be running. The agent publishes the IamAlive metric to Amazon CloudWatch every 30 seconds. An alarm is</p> <p>Log in to the host and make sure that the RDS Custom agent is running.</p> <p>You can use the following commands to find the agent's status.</p>

Notification	Description	Action
<p>[i-XXXXXXXXXXXXXXXXXX] has changed from RUNNING to STOPPED.</p>	<p>triggered if the metric hasn't been published for 30 seconds.</p> <p>The support perimeter also monitors the RDS Custom agent process state on the host every 30 minutes.</p> <p>On RDS Custom for Oracle, the DB instance goes outside the support perimeter if the RDS Custom agent stops.</p>	<pre>ps -ef grep RDSCustomAgent</pre> <pre>pgrep java</pre> <p>When the RDS Custom agent is running again, the IamAlive metric is published to Amazon CloudWatch, and the alarm switches to the OK state. This switch notifies the support perimeter that the agent is running.</p>
<p>RDS Custom agent status (RDS Custom for SQL Server):</p> <p>The RDS Custom instance is going out of perimeter because an unsupported configuration was used for RDS Custom agent.</p>	<p>The RDS Custom agent must always be running.</p> <p>The support perimeter monitors the RDS Custom agent process state on the host every 1 minute.</p> <p>On RDS Custom for SQL Server, a stopped agent is recovered by the monitoring service. The DB instance goes outside the support perimeter if the RDS Custom agent is uninstalled.</p>	<p>Log in to the host and make sure that the RDS Custom agent is running.</p> <p>You can use the following commands to find the agent's status.</p> <pre>\$name = "RDSCustomAgent" \$service = Get-Service \$name Write-Host \$service.Status</pre> <p>If the status isn't Running, you can start the service with the following command:</p> <pre>Start-Service \$name</pre>
<p>AWS Systems Manager agent (SSM agent) status (RDS Custom for Oracle):</p> <p>The AWS Systems Manager agent on EC2 instance [i-XXXXXXXXXXXXXXXXXX] is currently unreachable. Make sure you have correctly configured the network, agent, and IAM permissions.</p>	<p>The SSM agent must always be running. The RDS Custom agent is responsible for making sure that the Systems Manager agent is running.</p> <p>If the SSM agent was down and restarted, the RDS Custom agent publishes a metric to CloudWatch. The RDS Custom agent has an alarm on the metric set to trigger when there has been a restart in each of the previous three minutes.</p> <p>The support perimeter also monitors the SSM agent process state on the host every 30 minutes.</p>	<p>For more information, see Troubleshooting SSM Agent.</p> <p>When the SSM agent is running again, the alarm switches to the OK state. This switch notifies the support perimeter that the agent is running.</p>

Notification	Description	Action
<p>SSM agent status (RDS Custom for SQL Server):</p> <p>The RDS Custom instance is going out of perimeter because an unsupported configuration was used for SSM agent.</p>	<p>The SSM agent must always be running. The RDS Custom agent is responsible for making sure that the Systems Manager agent is running.</p> <p>The support perimeter monitors the SSM agent process state on the host every 1 minute.</p>	<p>For more information, see Troubleshooting SSM Agent.</p>
<p>sudo configurations (RDS Custom for Oracle only):</p> <p>The sudo configurations on EC2 instance [i-xxxxxxxxxxxxxxxxxx] have changed.</p>	<p>The support perimeter monitors that certain OS users are allowed to run certain commands on the box. It monitors sudo configurations against the supported state.</p> <p>When the sudo configurations aren't supported, the RDS Custom tries to overwrite them back to the previous supported state. If that is successful, the following notification is sent:</p> <p>RDS Custom successfully overwrote your configuration.</p>	<p>If the overwrite is unsuccessful, you can log in to the host and investigate why recent changes to the sudo configurations aren't supported.</p> <p>You can use the following command.</p> <pre data-bbox="904 756 1480 825"><code>visudo -c -f /etc/sudoers.d/<i>individual_sudo_files</i></code></pre> <p>After the support perimeter determines that the sudo configurations are supported, the DB instance becomes available within 30 minutes.</p>

Notification	Description	Action
<p>Amazon Elastic Block Store (Amazon EBS) volumes:</p> <p>RDS Custom for Oracle:</p> <ul style="list-style-type: none"> The following Amazon EBS volumes are attached to Amazon EC2 instance [i-xxxxxxxxxxxxxxxxxxxx]: [[vol- <i>01234abcd56789ef0</i>, vol- <i>0def6789abcd01234</i>]]. The original Amazon EBS volumes attached to Amazon EC2 instance [i-xxxxxxxxxxxxxxxxxxxx] have been detached or modified. You can't attach or modify the initial EBS volumes attached to an RDS Custom instance. <p>RDS Custom for SQL Server:</p> <ul style="list-style-type: none"> The RDS Custom instance is going out of perimeter because an unsupported configuration was used for EBS volume metadata. 	<p>RDS Custom creates two types of EBS volume, besides the root volume created from the Amazon Machine Image (AMI), and associates them with the EC2 instance.</p> <p>The binary volume is where the database software binaries are located. The data volumes are where database files are located. The storage configurations that you set when creating the DB instance are used to configure the data volumes.</p> <p>The support perimeter monitors the following:</p> <ul style="list-style-type: none"> The initial EBS volumes created with the DB instance are still associated. The initial EBS volumes still have the same configurations as initially set: storage type, size, Provisioned IOPS, and storage throughput. (RDS Custom for Oracle only) No additional EBS volumes are attached to the DB instance. 	<p>If you detached any initial EBS volumes, contact AWS Support.</p> <p>If you modified the storage type, Provisioned IOPS, or storage throughput of an EBS volume, revert the modification to the original value.</p> <p>If you modified the storage size of an EBS volume, contact AWS Support.</p> <p>(RDS Custom for Oracle only) If you attached any additional EBS volumes, do either of the following:</p> <ul style="list-style-type: none"> Detach the additional EBS volumes from the RDS Custom DB instance. Contact AWS Support.
<p>EBS-optimized instances (RDS Custom for Oracle only):</p> <p>The EBS-optimized attribute of Amazon EC2 instance [i-xxxxxxxxxxxxxxxxxxxx] has changed from [enabled] to [disabled].</p>	<p>Amazon EC2 instances should be EBS optimized.</p> <p>If the EBS-optimized attribute is turned off (disabled), the support perimeter doesn't put the DB instance into the unsupported-configuration state.</p>	<p>To turn on the EBS-optimized attribute:</p> <ol style="list-style-type: none"> Stop the EC2 instance. Set the EBS-optimized attribute to enabled. Start the EC2 instance. Remount the binary and data volumes.

Notification	Description	Action
<p>Amazon EC2 instance state:</p> <ul style="list-style-type: none"> The state of the EC2 instance [<i>i-XXXXXXXXXXXXXXXXXX</i>] has changed from [RUNNING] to [STOPPING]. The Amazon EC2 instance [<i>i-XXXXXXXXXXXXXXXXXX</i>] has been terminated and can't be found. Delete the database instance to clean up resources. The Amazon EC2 instance [<i>i-XXXXXXXXXXXXXXXXXX</i>] has been stopped. Start the instance, and restore the host configuration. For more information, see the troubleshooting documentation. 	<p>The support perimeter monitors EC2 instance state-change notifications. The EC2 instance must always be running.</p>	<p>If the EC2 instance is stopped, start it and remount the binary and data volumes.</p> <p>On RDS Custom for Oracle, if the EC2 instance is terminated, delete the RDS Custom DB instance.</p> <p>On RDS Custom for SQL Server, if the EC2 instance is terminated, RDS Custom performs an automated recovery to provision a new EC2 instance.</p>
<p>Amazon EC2 instance attributes:</p> <p>RDS Custom for Oracle:</p> <ul style="list-style-type: none"> The attributes of Amazon EC2 instance [<i>i-XXXXXXXXXXXXXXXXXX</i>] have changed. <p>RDS Custom for SQL Server:</p> <ul style="list-style-type: none"> The RDS Custom instance is going out of perimeter because an unsupported configuration was used for EC2 instance metadata. 	<p>The support perimeter monitors the instance type of the EC2 instance where the RDS Custom DB instance is running. The EC2 instance type must stay the same as when you set it up during RDS Custom DB instance creation.</p>	<p>Change the EC2 instance type back to the original type using the EC2 console or CLI.</p> <p>To change the instance type because of scaling requirements, do a PITR and specify the new instance type and class. However, doing this results in a new RDS Custom DB instance with a new host and Domain Name System (DNS) name.</p>
<p>Oracle Data Guard role (RDS Custom for Oracle only):</p> <ul style="list-style-type: none"> The instance role for DB instance <i>my-custom-instance</i> was changed. The database role [LOGICAL STANDBY] isn't supported. Validate the Oracle Data Guard configuration for the database on Amazon EC2 instance [<i>i-XXXXXXXXXXXXXXXXXX</i>]. 	<p>The support perimeter monitors the current database role every 15 seconds and sends a CloudWatch notification if the database role has changed.</p> <p>The Oracle Data Guard DATABASE_ROLE parameter must be either PRIMARY or PHYSICAL STANDBY.</p>	<p>Restore the Oracle Data Guard database role to a supported value.</p> <p>After the support perimeter determines that the database role is supported, the RDS Custom for Oracle DB instance becomes available within 15 seconds.</p>

Notification	Description	Action
<p>Shared memory connections (RDS Custom for SQL Server only):</p> <p>The RDS Custom instance is going out of perimeter because an unsupported configuration was used for shared memory protocol.</p>	<p>The RDS Custom agent on the EC2 host connects to SQL Server using the shared memory protocol.</p> <p>If this protocol is turned off (Enabled is set to No), then RDS Custom can't perform its management actions and places the DB instance outside the support perimeter.</p>	<p>To bring the RDS Custom for SQL Server DB instance back within the support perimeter, turn on the shared memory protocol on the Protocol page of the Shared Memory Properties window by setting Enabled to Yes.</p> <p>Restart SQL Server after enabling the protocol.</p>
<p>Database file locations (RDS Custom for SQL Server only):</p> <p>The RDS Custom instance is going out of perimeter because an unsupported configuration was used for database files location.</p>	<p>All SQL Server database files are stored on the D: drive by default, in the D:\rdsdbdata\DATA directory.</p> <p>If you create or alter the database file location to be anywhere other than the D: drive, then RDS Custom places the DB instance outside the support perimeter.</p> <p>We strongly recommend that you don't save any database files on the C: drive. You can lose data on the C: drive during certain operations, such as hardware failure. Storage on the C: drive doesn't offer the same durability as on the D: drive, which is an EBS volume.</p> <p>Also, if database files can't be found, RDS Custom places the DB instance outside the support perimeter.</p>	<p>Store all RDS Custom for SQL Server database files on the D: drive.</p>

How Amazon RDS Custom replaces an impaired host

If the Amazon EC2 host becomes impaired, RDS Custom attempts to reboot it. If this effort fails, RDS Custom uses the same stop and start feature included in Amazon EC2.

Topics

- [Stopping and starting the host \(p. 898\)](#)
- [Effects of host replacement \(p. 898\)](#)
- [Best practices for Amazon EC2 hosts \(p. 898\)](#)

Stopping and starting the host

RDS Custom automatically takes the following steps, with no user intervention required:

1. Stops the Amazon EC2 host.

The EC2 instance performs a normal shutdown and stops running. Any Amazon EBS volumes remain attached to the instance, and their data persists. Any data stored in the instance store volumes (not supported on RDS Custom) or RAM of the host computer is gone.

For more information, see [Stop and start your instance](#) in the *Amazon EC2 User Guide for Linux Instances*.

2. Starts the Amazon EC2 host.

The EC2 instance migrates to a new underlying host hardware. In some cases, the RDS Custom DB instance remains on the original host.

Effects of host replacement

In RDS Custom, you have full control over the root device volume and Amazon EBS storage volumes. The root volume can contain important data and configurations that you don't want to lose.

RDS Custom for Oracle retains all database and customer data after the operation, including root volume data. No user intervention is required. On RDS Custom for SQL Server, database data is retained, but any data on the C: drive, including operating system and customer data, is lost.

After the replacement process, the Amazon EC2 host has a new public IP address. The host retains the following:

- Instance ID
- Private IP addresses
- Elastic IP addresses
- Instance metadata
- Data storage volume data
- Root volume data (on RDS Custom for Oracle)

Best practices for Amazon EC2 hosts

The Amazon EC2 host replacement feature covers the majority of Amazon EC2 impairment scenarios. We recommend that you adhere to the following best practices:

- Before you change your configuration or the operating system, back up your data. If the root volume or operating system becomes corrupt, host replacement can't repair it. Your only options are restoring from a DB snapshot or point-in-time recovery.
- Don't manually stop or terminate the physical Amazon EC2 host. Both actions result in the instance being put outside the RDS Custom support perimeter.
- (RDS Custom for SQL Server) If you attach additional volumes to the Amazon EC2 host, configure them to remount upon restart. If the host is impaired, RDS Custom might stop and start the host automatically.

Troubleshooting upgrades for RDS Custom for Oracle

Your upgrade of an RDS Custom for Oracle instance might fail. Following, you can find techniques that you can use during upgrades of RDS Custom DB for Oracle DB instances:

- Examine the following log files:
 - All upgrade output log files reside in the /tmp directory on the DB instance.
 - These log files are named catupg*.log.
 - A master output file named /tmp/catupgrd0.log reports all errors, and the steps performed.
 - The alert.log file for the DB instance is located in the /rdsdbdata/log/trace directory. Examine this file regularly as a best practice.
- Run the following grep command in the root directory to track the upgrade OS process. This command shows where the log files are being written and determine the state of the upgrade process.

```
ps -aux | grep upg
```

The output resembles the following.

```
root      18884  0.0  0.0 235428  8172 ?        S<   17:03   0:00 /usr/bin/sudo -u rdsdb /rdsdbbin/scripts/oracle-control ORCL op_apply_upgrade_sh RDS-UPGRADE/2.upgrade.sh
rdsdb    18886  0.0  0.0 153968 12164 ?        S<   17:03   0:00 /usr/bin/perl -T -w /rdsdbbin/scripts/oracle-control ORCL op_apply_upgrade_sh RDS-UPGRADE/2.upgrade.sh
rdsdb    18887  0.0  0.0 113196  3032 ?        S<   17:03   0:00 /bin/sh /rdsdbbin/oracle/rdbms/admin/RDS-UPGRADE/2.upgrade.sh
rdsdb    18900  0.0  0.0 113196  1812 ?        S<   17:03   0:00 /bin/sh /rdsdbbin/oracle/rdbms/admin/RDS-UPGRADE/2.upgrade.sh
rdsdb    18901  0.1  0.0 167652  20620 ?        S<   17:03   0:07 /rdsdbbin/oracle/perl/bin/perl catctl.pl -n 4 -d /rdsdbbin/oracle/rdbms/admin -l /tmp catupgrd.sql
root      29944  0.0  0.0 112724  2316 pts/0    S+   18:43   0:00 grep --color=auto upg
```

- Run the following SQL query to verify the current state of the components to find the database version and the options installed on the DB instance.

```
set linesize 180
column comp_id format a15
column comp_name format a40 trunc
column status format a15 trunc
select comp_id, comp_name, version, status from dba_registry order by 1;
```

The output resembles the following.

COMP_NAME	STATUS	PROCEDURE
-----	-----	-----
Oracle Database Catalog Views	VALID	
DBMS_REGISTRY_SYS.VALIDATE_CATALOG		
Oracle Database Packages and Types	VALID	
DBMS_REGISTRY_SYS.VALIDATE_CATPROC		
Oracle Text	VALID	VALID_CONTEXT
Oracle XML Database	VALID	DBMS_REGXDB.VALIDATEXDB
4 rows selected.		

- Run the following SQL query to check for invalid objects that might interfere with the upgrade process.

```
set pages 1000 lines 2000
```

```
col OBJECT for a40
Select substr(owner,1,12) owner,
       substr(object_name,1,30) object,
       substr(object_type,1,30) type, status,
       created
  from
    dba_objects where status <>'VALID' and owner in ('SYS','SYSTEM','RDSADMIN','XDB');
```

Troubleshooting replica promotion for RDS Custom for Oracle

You can promote managed Oracle replicas in RDS Custom for Oracle using the console, `promote-read-replica` AWS CLI command, or `PromoteReadReplica` API. If you delete your primary DB instance, and all replicas are healthy, RDS Custom for Oracle promotes your managed replicas to standalone instances automatically. If a replica has paused automation or is outside the support perimeter, you must fix the replica before RDS Custom can promote it automatically. For more information, see [Replica promotion requirements and limitations \(p. 829\)](#).

The replica promotion workflow might become stuck in the following situation:

- The primary DB instance is in the state `STORAGE_FULL`.
- The primary DB can't archive all of its online redo logs.
- A gap exists between the archived redo log files on your Oracle replica and the primary database.

To respond to the stuck workflow, complete the following steps:

1. Synchronize the redo log gap on your Oracle replica DB instance.
2. Force the promotion of your read replica to the latest applied redo log. Run the following commands in SQL*Plus:

```
ALTER DATABASE ACTIVATE STANDBY DATABASE;
SHUTDOWN IMMEDIATE
STARTUP
```

3. Contact AWS Support and request it to move your DB instance to available status.

Troubleshooting replica creation for RDS Custom for Oracle

When you attempt to create a new Oracle replica from an RDS Custom for Oracle DB instance that was created before November 18, 2022, the replication becomes stuck. You can fix this problem by creating a new SPFILE on the Oracle replica that is experiencing the problem.

To create a new SPFILE on your Oracle replica

1. Log in to the underlying Amazon EC2 instance for your Oracle replica. Use `sed` to change the current Oracle home value of `/rdsdbbin/oracle` to the latest Oracle home in your initialization parameter file.

```
sed -i "s|/rdsdbbin/oracle|${ORACLE_HOME}|g" /rdsdbdata/config/oracle_pfile
```

2. Start an Oracle SQL client, and log in to your RDS Custom for Oracle DB instance as a user with SYSDBA privileges.
3. In your SQL client, create an SPFILE from your initialization parameter file.

```
CREATE SPFILE='/rdsdbdata/admin/$ORACLE_SID/pfile/spfile$ORACLE_SID.ora'  
FROM PFILE='/rdsdbdata/config/oracle_pfile';
```

4. Shut down your Oracle replica database:

```
SHUTDOWN IMMEDIATE
```

5. Start your Oracle replica database and mount it:

```
STARTUP MOUNT
```

Your source RDS Custom for Oracle DB instance can now replicate to your Oracle replica database.

Working with Amazon RDS on AWS Outposts

Amazon RDS on AWS Outposts extends RDS for SQL Server, RDS for MySQL, and RDS for PostgreSQL databases to AWS Outposts environments. AWS Outposts uses the same hardware as in public AWS Regions to bring AWS services, infrastructure, and operation models on-premises. With RDS on Outposts, you can provision managed DB instances close to the business applications that must run on-premises. For more information about AWS Outposts, see [AWS Outposts](#).

You use the same AWS Management Console, AWS CLI, and RDS API to provision and manage on-premises RDS on Outposts DB instances as you do for RDS DB instances running in the AWS Cloud. RDS on Outposts automates tasks, such as database provisioning, operating system and database patching, backup, and long-term archival in Amazon S3.

RDS on Outposts supports automated backups of DB instances. Network connectivity between your Outpost and your AWS Region is required to back up and restore DB instances. All DB snapshots and transaction logs from an Outpost are stored in your AWS Region. From your AWS Region, you can restore a DB instance from a DB snapshot to a different Outpost. For more information, see [Working with backups \(p. 427\)](#).

RDS on Outposts supports automated maintenance and upgrades of DB instances. For more information, see [Maintaining a DB instance \(p. 350\)](#).

RDS on Outposts uses encryption at rest for DB instances and DB snapshots using your AWS KMS key. For more information about encryption at rest, see [Encrypting Amazon RDS resources \(p. 2000\)](#).

By default, EC2 instances in Outposts subnets can use the Amazon Route 53 DNS Service to resolve domain names to IP addresses. You might encounter longer DNS resolution times with Route 53, depending on the path latency between your Outpost and the AWS Region. In such cases, you can use the DNS servers installed locally in your on-premises environment. For more information, see [DNS](#) in the [AWS Outposts User Guide](#).

When network connectivity to the AWS Region isn't available, your DB instance continues to run locally. You can continue to access DB instances using DNS name resolution by configuring a local DNS server as a secondary server. However, you can't create new DB instances or take new actions on existing DB instances. Automatic backups don't occur when there is no connectivity. If there is a DB instance failure, the DB instance isn't automatically replaced until connectivity is restored. We recommend restoring network connectivity as soon as possible.

Topics

- [Prerequisites for Amazon RDS on AWS Outposts \(p. 902\)](#)
- [Amazon RDS on AWS Outposts support for Amazon RDS features \(p. 904\)](#)
- [Supported DB instance classes for Amazon RDS on AWS Outposts \(p. 907\)](#)
- [Customer-owned IP addresses for Amazon RDS on AWS Outposts \(p. 909\)](#)
- [Working with Multi-AZ deployments for Amazon RDS on AWS Outposts \(p. 911\)](#)
- [Creating DB instances for Amazon RDS on AWS Outposts \(p. 914\)](#)
- [Considerations for restoring DB instances on Amazon RDS on AWS Outposts \(p. 920\)](#)

Prerequisites for Amazon RDS on AWS Outposts

The following are prerequisites for using Amazon RDS on AWS Outposts:

- Install AWS Outposts in your on-premises data center. For more information about AWS Outposts, see [AWS Outposts](#).
- Make sure that you have at least one subnet available for RDS on Outposts. You can use the same subnet for other workloads.
- Make sure that you have a reliable network connection between your Outpost and an AWS Region.

Amazon RDS on AWS Outposts support for Amazon RDS features

The following table describes the Amazon RDS features supported by Amazon RDS on AWS Outposts.

Feature	Supported	Notes	More information
DB instance provisioning	Yes	You can only create DB instances for RDS for SQL Server, RDS for MySQL, and RDS for PostgreSQL DB engines. The following versions are supported: <ul style="list-style-type: none"> Microsoft SQL Server: <ul style="list-style-type: none"> 15.00.4043.16.v1 and higher 2019 versions 14.00.3294.2.v1 and higher 2017 versions 13.00.5820.21.v1 and higher 2016 versions MySQL version 8.0.23 and higher MySQL 8.0 versions All PostgreSQL 14 & 13 versions, and PostgreSQL version 12.5 and higher PostgreSQL 12 versions 	Creating DB instances for Amazon RDS on AWS Outposts (p. 914)
Connect to a Microsoft SQL Server DB instance with Microsoft SQL Server Management Studio	Yes	Some TLS versions and encryption ciphers might not be secure. To turn them off, follow the instructions in Configuring security protocols and ciphers (p. 1138) .	Connecting to a DB instance running the Microsoft SQL Server database engine (p. 1084)
Modifying the master user password	Yes	—	Modifying an Amazon RDS DB instance (p. 327)
Renaming a DB instance	Yes	—	Modifying an Amazon RDS DB instance (p. 327)
Rebooting a DB instance	Yes	—	Rebooting a DB instance (p. 366)
Stopping a DB instance	Yes	—	Stopping an Amazon RDS DB instance temporarily (p. 317)
Starting a DB instance	Yes	—	Starting an Amazon RDS DB instance that was previously stopped (p. 320)

Feature	Supported	Notes	More information
Multi-AZ deployments	Yes	Multi-AZ deployments are supported on MySQL and PostgreSQL DB instances.	Creating DB instances for Amazon RDS on AWS Outposts (p. 914) Multi-AZ deployments for high availability (p. 121)
DB parameter groups	Yes	—	Working with parameter groups (p. 289)
Read replicas	No	—	Working with read replicas (p. 370)
Encryption at rest	Yes	RDS on Outposts doesn't support unencrypted DB instances.	Encrypting Amazon RDS resources (p. 2000)
AWS Identity and Access Management (IAM) database authentication	No	—	IAM database authentication for MariaDB, MySQL, and PostgreSQL (p. 2048)
Associating an IAM role with a DB instance	No	—	add-role-to-db-instance AWS CLI command AddRoleToDBInstance RDS API operation
Kerberos authentication	No	—	Kerberos authentication (p. 1999)
Tagging Amazon RDS resources	Yes	—	Tagging Amazon RDS resources (p. 392)
Option groups	Yes	—	Working with option groups (p. 273)
Modifying the maintenance window	Yes	—	Maintaining a DB instance (p. 350)
Automatic minor version upgrade	Yes	—	Automatically upgrading the minor engine version (p. 362)
Modifying the backup window	Yes	—	Working with backups (p. 427) Modifying an Amazon RDS DB instance (p. 327)
Changing the DB instance class	Yes	—	Modifying an Amazon RDS DB instance (p. 327)
Changing the allocated storage	Yes	—	Modifying an Amazon RDS DB instance (p. 327)

Feature	Supported	Notes	More information
Storage autoscaling	Yes	—	Managing capacity automatically with Amazon RDS storage autoscaling (p. 412)
Manual and automatic DB instance snapshots	Yes	<p>You can store automated backups and manual snapshots in your AWS Region. Or you can store them locally on your Outpost.</p> <p>Local backups are supported on MySQL and PostgreSQL DB instances.</p> <p>To store backups on your Outpost, make sure that you have Amazon S3 on Outposts configured.</p>	Creating DB instances for Amazon RDS on AWS Outposts (p. 914) Amazon S3 on Outposts Creating a DB snapshot (p. 448)
Restoring from a DB snapshot	Yes	You can store automated backups and manual snapshots for the restored DB instance in the parent AWS Region or locally on your Outpost.	Considerations for restoring DB instances on Amazon RDS on AWS Outposts (p. 920) Restoring from a DB snapshot (p. 452)
Restoring a DB instance from Amazon S3	No	—	Restoring a backup into a MySQL DB instance (p. 1361)
Exporting snapshot data to Amazon S3	No	—	Exporting DB snapshot data to Amazon S3 (p. 481)
Point-in-time recovery	Yes	You can store automated backups and manual snapshots for the restored DB instance in the parent AWS Region or locally on your Outpost, with one exception.	Considerations for restoring DB instances on Amazon RDS on AWS Outposts (p. 920) Restoring a DB instance to a specified time (p. 499)
Enhanced monitoring	No	—	Monitoring OS metrics with Enhanced Monitoring (p. 600)
Amazon CloudWatch monitoring	Yes	You can view the same set of metrics that are available for your databases in the AWS Region.	Monitoring Amazon RDS metrics with Amazon CloudWatch (p. 528)
Publishing database engine logs to CloudWatch Logs	Yes	—	Publishing database logs to Amazon CloudWatch Logs (p. 683)

Feature	Supported	Notes	More information
Event notification	Yes	—	Working with Amazon RDS event notification (p. 650)
Amazon RDS Performance Insights	No	—	Monitoring DB load with Performance Insights on Amazon RDS (p. 543)
Viewing or downloading database logs	No	<p>RDS on Outposts doesn't support viewing database logs using the console or describing database logs using the AWS CLI or RDS API.</p> <p>RDS on Outposts doesn't support downloading database logs using the console or downloading database logs using the AWS CLI or RDS API.</p>	Monitoring Amazon RDS log files (p. 680)
Amazon RDS Proxy	No	—	Using Amazon RDS Proxy (p. 921)
Stored procedures for Amazon RDS for MySQL	Yes	—	MySQL on Amazon RDS SQL reference (p. 1439)
Replication with external databases for RDS for MySQL	No	—	Configuring binary log file position replication with an external source instance (p. 1408)
Native backup and restore for Amazon RDS for Microsoft SQL Server	Yes	—	Importing and exporting SQL Server databases using native backup and restore (p. 1099)

Supported DB instance classes for Amazon RDS on AWS Outposts

Amazon RDS on AWS Outposts supports the following DB instance classes:

- General purpose DB instance classes
 - db.m5.24xlarge
 - db.m5.12xlarge
 - db.m5.4xlarge
 - db.m5.2xlarge
 - db.m5.xlarge
 - db.m5.large
- Memory optimized DB instance classes

- db.r5.24xlarge
- db.r5.12xlarge
- db.r5.4xlarge
- db.r5.2xlarge
- db.r5.xlarge
- db.r5.large

Depending on how you've configured your Outpost, you might not have all of these classes available. For example, if you haven't purchased the db.r5 classes for your Outpost, you can't use them with RDS on Outposts.

Only general purpose SSD storage is supported for RDS on Outposts DB instances. For more information about DB instance classes, see [DB instance classes \(p. 10\)](#).

Amazon RDS manages maintenance and recovery for your DB instances and requires active capacity on the Outpost to do so. We recommend that you configure N+1 EC2 instances for each DB instance class in your production environments. RDS on Outposts can use the extra capacity of these EC2 instances for maintenance and repair operations. For example, if your production environments have 3 db.m5.large and 5 db.r5.xlarge DB instance classes, then we recommend that they have at least 4 m5.large EC2 instances and 6 r5.xlarge EC2 instances. For more information, see [Resilience in AWS Outposts](#) in the [AWS Outposts User Guide](#).

Customer-owned IP addresses for Amazon RDS on AWS Outposts

Amazon RDS on AWS Outposts uses information that you provide about your on-premises network to create an address pool. This pool is known as a *customer-owned IP address pool* (CoIP pool). *Customer-owned IP addresses* (CoIPs) provide local or external connectivity to resources in your Outpost subnets through your on-premises network. For more information about CoIPs, see [Customer-owned IP addresses](#) in the *AWS Outposts User Guide*.

Each RDS on Outposts DB instance has a private IP address for traffic inside its virtual private cloud (VPC). This private IP address isn't publicly accessible. You can use the **Public** option to set whether the DB instance also has a public IP address in addition to the private IP address. Using the public IP address for connections routes them through the internet and can result in high latencies in some cases.

Instead of using these private and public IP addresses, RDS on Outposts supports using CoIPs for DB instances through their subnets. When you use a CoIP for an RDS on Outposts DB instance, you connect to the DB instance with the DB instance endpoint. RDS on Outposts then automatically uses the CoIP for all connections from both inside and outside of the VPC.

CoIPs can provide the following benefits for RDS on Outposts DB instances:

- Lower connection latency
- Enhanced security

Using CoIPs

You can turn CoIPs on or off for an RDS on Outposts DB instance using the AWS Management Console, the AWS CLI, or the RDS API:

- With the AWS Management Console, choose the **Customer-owned IP address (CoIP)** setting in **Access type** to use CoIPs. Choose one of the other settings to turn them off.

▼ Additional configuration

Access type [Info](#)

Private

RDS will not assign a public IP address to the database. Amazon EC2 instances and devices inside the VPC can connect to your database. EC2 instances and devices outside your VPC can't connect unless they use AWS Site-to-Site VPN or AWS Direct Connect.

Customer-owned IP address (CoIP)

Devices on your on-premises network can connect to your database through a CoIP.

Public

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices can connect to the database.

Database port

TCP/IP port that the database will use for application connections.

3306

- With the AWS CLI, use the `--enable-customer-owned-ip` | `--no-enable-customer-owned-ip` option.
- With the RDS API, use the `EnableCustomerOwnedIp` parameter.

You can turn CoIPs on or off when you perform any of the following actions:

- Create a DB instance

For more information, see [Creating DB instances for Amazon RDS on AWS Outposts \(p. 914\)](#).

- Modify a DB instance

For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- Restore a DB instance from a snapshot

For more information, see [Restoring from a DB snapshot \(p. 452\)](#).

- Restore a DB instance to a specified time

For more information, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Note

In some cases, you might turn on CoIPs for a DB instance but Amazon RDS isn't able to allocate a CoIP for the DB instance. In such cases, the DB instance status is changed to **incompatible-network**. For more information about the DB instance status, see [Viewing Amazon RDS DB instance status \(p. 516\)](#).

Limitations

The following limitations apply to CoIP support for RDS on Outposts DB instances:

- When using a CoIP for a DB instance, make sure that public accessibility is turned off for that DB instance.
- Make sure that the inbound rules for your VPC security groups include the CoIP address range (CIDR block). For more information about setting up security groups, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).
- You can't assign a CoIP from a CoIP pool to a DB instance. When you use a CoIP for a DB instance, Amazon RDS automatically assigns a CoIP from a CoIP pool to the DB instance.
- You must use the AWS account that owns the Outpost resources (owner) or share the following resources with other AWS accounts (consumers) in the same organization:
 - The Outpost
 - The local gateway (LGW) route table for the DB instance's VPC
 - The CoIP pool or pools for the LGW route table

For more information, see [Working with shared AWS Outposts resources](#) in the *AWS Outposts User Guide*.

Working with Multi-AZ deployments for Amazon RDS on AWS Outposts

For Multi-AZ deployments, Amazon RDS creates a primary DB instance on one AWS Outpost. RDS synchronously replicates the data to a standby DB instance on a different Outpost.

Multi-AZ deployments on AWS Outposts operate like Multi-AZ deployments in AWS Regions, but with the following differences:

- They require a local connection between two or more Outposts.
- They require customer-owned IP (CoIP) pools. For more information, see [Customer-owned IP addresses for Amazon RDS on AWS Outposts \(p. 909\)](#).
- Replication runs on your local network.

Multi-AZ on AWS Outposts is available for all supported versions of MySQL and PostgreSQL on RDS on Outposts. Local backups aren't supported for Multi-AZ deployments. For more information, see [Creating DB instances for Amazon RDS on AWS Outposts \(p. 914\)](#).

Working with the shared responsibility model

Although AWS uses commercially reasonable efforts to provide DB instances configured for high availability, the availability uses a shared responsibility model. The ability of RDS on Outposts to fail over and repair DB instances requires each of your Outposts to be connected to its AWS Region.

RDS on Outposts also requires connectivity between the Outpost that is hosting the primary DB instance and the Outpost that is hosting the standby DB instance for synchronous replication. Any impact to this connection can prevent RDS on Outposts from performing a failover.

You might see elevated latencies for a standard DB instance deployment as a result of the synchronous data replication. The bandwidth and latency of the connection between the Outpost hosting the primary DB instance and the Outpost hosting the standby DB instance directly affect latencies. For more information, see [Prerequisites \(p. 912\)](#).

Improving availability

We recommend the following actions to improve availability:

- Allocate enough additional capacity for your mission-critical applications to allow recovery and failover if there is an underlying host issue. This applies to all Outposts that contain subnets in your DB subnet group. For more information, see [Resilience in AWS Outposts](#).
- Create multiple connections from each of your Outposts to the AWS Region.
- Use more than two Outposts. Having more than two Outposts allows Amazon RDS to recover a DB instance. RDS does this recovery by moving the DB instance to another Outpost if the current Outpost experiences a failure.
- Provide dual power sources and redundant network connectivity for your Outpost.

We recommend the following for your local networks:

- The round trip time (RTT) latency between the Outpost hosting your primary DB instance and the Outpost hosting your standby DB instance directly affects write latency. Keep the RTT latency between the AWS Outposts in the low single-digit milliseconds. We recommend not more than 5 milliseconds, but your requirements might vary.

You can find the net impact to network latency in the Amazon CloudWatch metrics for `WriteLatency`. For more information, see [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).

- The availability of the connection between the Outposts affects the overall availability of your DB instances. Have redundant network connectivity between the Outposts.

Prerequisites

Multi-AZ deployments on RDS on Outposts have the following prerequisites:

- Have at least two Outposts, connected over local connections and attached to different Availability Zones in an AWS Region.
- Make sure that your DB subnet groups contain the following:
 - At least two subnets in at least two Availability Zones in a given AWS Region.
 - Subnets only in Outposts.
 - At least two subnets in at least two Outposts within the same virtual private cloud (VPC).
- Associate your DB instance's VPC with all of your local gateway route tables. This association is necessary because replication runs over your local network using your Outposts' local gateways.

For example, suppose that your VPC contains subnet-A in Outpost-A and subnet-B in Outpost-B. Outpost-A uses LocalGateway-A (LGW-A), and Outpost-B uses LocalGateway-B (LGW-B). LGW-A has RouteTable-A, and LGW-B has RouteTable-B. You want to use both RouteTable-A and RouteTable-B for replication traffic. To do this, associate your VPC with both RouteTable-A and RouteTable-B.

For more information about how to create an association, see the Amazon EC2 [create-local-gateway-route-table-vpc-association](#) AWS CLI command.

- Make sure that your Outposts use customer-owned IP (CoIP) routing. Each route table must also each have at least one address pool. Amazon RDS allocates an additional IP address each for the primary and standby DB instances for data synchronization.
- Make sure that the AWS account that owns the RDS DB instances owns the local gateway route tables and CoIP pools. Or make sure it's part of a Resource Access Manager share with access to the local gateway route tables and CoIP pools.
- Make sure that the IP addresses in your CoIP pools can be routed from one Outpost local gateway to the others.
- Make sure that the VPC's CIDR blocks (for example, 10.0.0.0/4) and your CoIP pool CIDR blocks don't contain IP addresses from Class E (240.0.0.0/4). RDS uses these IP addresses internally.
- Make sure that you correctly set up outbound and related inbound traffic.

RDS on Outposts establishes a virtual private network (VPN) connection between the primary and standby DB instances. For this to work correctly, your local network must allow outbound and related inbound traffic for Internet Security Association and Key Management Protocol (ISAKMP). It does so using User Datagram Protocol (UDP) port 500 and IP Security (IPsec) Network Address Translation Traversal (NAT-T) using UDP port 4500.

For more information on CoIPs, see [Customer-owned IP addresses for Amazon RDS on AWS Outposts \(p. 909\)](#) in this guide, and [Customer-owned IP addresses](#) in the [AWS Outposts User Guide](#).

Working with API operations for Amazon EC2 permissions

Regardless of whether you use CoIPs for your DB instance on AWS Outposts, RDS requires access to your CoIP pool resources. RDS can call the following EC2 permissions API operations for CoIPs on your behalf for Multi-AZ deployments:

- `CreateCoipPoolPermission` – When you create a Multi-AZ DB instance on RDS on Outposts
- `DeleteCoipPoolPermission` – When you delete a Multi-AZ DB instance on RDS on Outposts

These API operations grant to, or remove from, internal RDS accounts the permission to allocate elastic IP addresses from the CoIP pool specified by the permission. You can view these IP addresses using the `DescribeCoipPoolUsage` API operation. For more information on CoIPs, see [Customer-owned IP addresses for Amazon RDS on AWS Outposts \(p. 909\)](#) and [Customer-owned IP addresses in the AWS Outposts User Guide](#).

RDS can also call the following EC2 permission API operations for local gateway route tables on your behalf for Multi-AZ deployments:

- `CreateLocalGatewayRouteTablePermission` – When you create a Multi-AZ DB instance on RDS on Outposts
- `DeleteLocalGatewayRouteTablePermission` – When you delete a Multi-AZ DB instance on RDS on Outposts

These API operations grant to, or remove from, internal RDS accounts the permission to associate internal RDS VPCs with your local gateway route tables. You can view these route table–VPC associations using the `DescribeLocalGatewayRouteTableVpcAssociations` API operations.

Creating DB instances for Amazon RDS on AWS Outposts

Creating an Amazon RDS on AWS Outposts DB instance is similar to creating an Amazon RDS DB instance in the AWS Cloud. However, make sure that you specify a DB subnet group that is associated with your Outpost.

A virtual private cloud (VPC) based on the Amazon VPC service can span all of the Availability Zones in an AWS Region. You can extend any VPC in the AWS Region to your Outpost by adding an Outpost subnet. To add an Outpost subnet to a VPC, specify the Amazon Resource Name (ARN) of the Outpost when you create the subnet.

Before you create an RDS on Outposts DB instance, you can create a DB subnet group that includes one subnet that is associated with your Outpost. When you create an RDS on Outposts DB instance, specify this DB subnet group. You can also choose to create a new DB subnet group when you create your DB instance.

For information about configuring AWS Outposts, see the [AWS Outposts User Guide](#).

Console

Creating a DB subnet group

Create a DB subnet group with one subnet that is associated with your Outpost.

You can also create a new DB subnet group for the Outpost when you create your DB instance. If you want to do so, then skip this procedure.

Note

To create a DB subnet group for the AWS Cloud, specify at least two subnets.

To create a DB subnet group for your Outpost

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region where you want to create the DB subnet group.
3. Choose **Subnet groups**, and then choose **Create DB Subnet Group**.

The **Create DB subnet group** page appears.

Create DB Subnet Group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

(Optional)

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Choose a VPC

Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

4. For **Name**, choose the name of the DB subnet group.
5. For **Description**, choose a description for the DB subnet group.
6. For **VPC**, choose the VPC that you're creating the DB subnet group for.
7. For **Availability Zones**, choose the Availability Zone for your Outpost.
8. For **Subnets**, choose the subnet for use by RDS on Outposts.
9. Choose **Create** to create the DB subnet group.

Creating the RDS on Outposts DB instance

Create the DB instance, and choose the Outpost for your DB instance.

To create an RDS on Outposts DB instance using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the Amazon RDS console, choose the AWS Region where the Outpost on which you want to create the DB instance is attached.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.

The AWS Management Console detects available Outposts that you have configured and presents the **On-premises** option in the **Database location** section.

Note

If you haven't configured any Outposts, either the **Database location** section doesn't appear or the **RDS on Outposts** option isn't available in the **Choose an on-premises creation method** section.

5. For **Database location**, choose **On-premises**.
6. For **On-premises creation method**, choose **RDS on Outposts**.
7. Specify your settings for **Outposts Connectivity**. These settings are for the Outpost that uses the VPC that has the DB subnet group for your DB instance. Your VPC must be based on the Amazon VPC service.
 - a. For **Virtual Private Cloud (VPC)**, choose the VPC that contains the DB subnet group for your DB instance.
 - b. For **VPC security group**, choose the Amazon VPC security group for your DB instance.
 - c. For **DB subnet group**, choose the DB subnet group for your DB instance.

You can choose an existing DB subnet group that's associated with the Outpost—for example, if you performed the procedure in [Creating a DB subnet group \(p. 914\)](#).

You can also create a new DB subnet group for the Outpost.

8. For **Multi-AZ deployment**, choose **Create a standby instance (recommended for production usage)** to create a standby DB instance in another Outpost.

Note

This option isn't available for Microsoft SQL Server.

If you choose to create a Multi-AZ deployment, you can't store backups on your Outpost.

9. Under **Backup**, do the following:

- a. For **Backup target**, choose one of the following:
 - **AWS Cloud** to store automated backups and manual snapshots in the parent AWS Region.
 - **Outposts (on-premises)** to create local backups.

Note

To store backups on your Outpost, your Outpost must have Amazon S3 capability.

For more information, see [Amazon S3 on Outposts](#).

Local backups aren't supported for Multi-AZ deployments.

- b. Choose **Enable automated backups** to create point-in-time snapshots of your DB instance.

If you turn on automated backups, then you can choose values for **Backup retention period** and **Backup window**, or leave the default values.

10. Specify other DB instance settings as needed.

For information about each setting when creating a DB instance, see [Settings for DB instances \(p. 237\)](#).

11. Choose **Create database**.

The **Databases** page appears. A banner tells you that your DB instance is being created, and displays the **View credential details** button.

Viewing DB instance details

After you create your DB instance, you can view credentials and other details for it.

To view DB instance details

1. To view the master user name and password for the DB instance, choose **View credential details** on the **Databases** page.

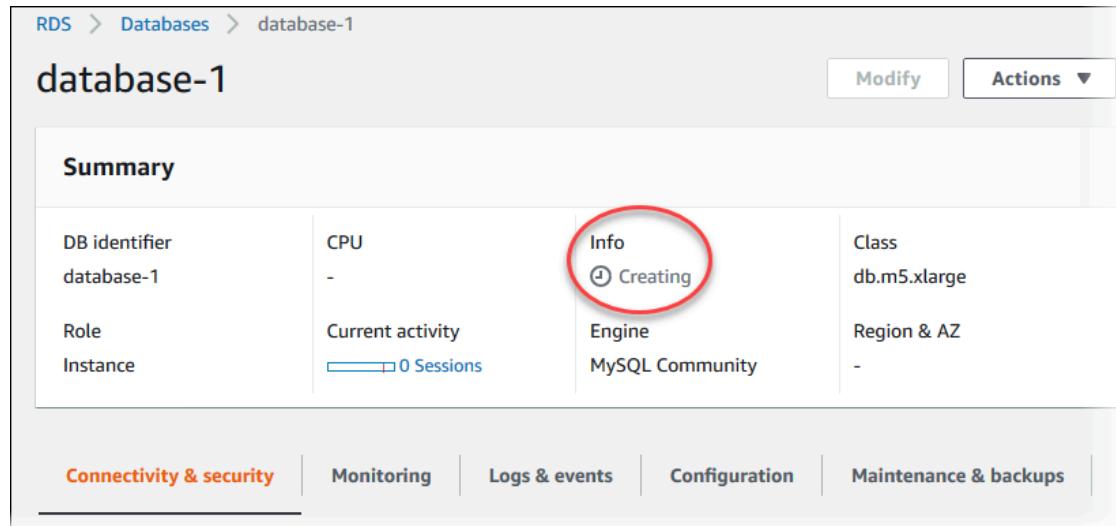
You can connect to the DB instance as the master user by using these credentials.

Important

You can't view the master user password again. If you don't record it, you might have to change it. To change the master user password after the DB instance is available, modify the DB instance. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

2. Choose the name of the new DB instance on the **Databases** page.

On the RDS console, the details for the new DB instance appear. The DB instance has a status of **Creating** until the DB instance is created and ready for use. When the state changes to **Available**, you can connect to the DB instance. Depending on the DB instance class and storage allocated, it can take several minutes for the new DB instance to be available.



After the DB instance is available, you can manage it the same way that you manage RDS DB instances in the AWS Cloud.

AWS CLI

Before you create a new DB instance in an Outpost with the AWS CLI, first create a DB subnet group for use by RDS on Outposts.

To create a DB subnet group for your Outpost

- Use the [create-db-subnet-group](#) command. For `--subnet-ids`, specify the subnet group in the Outpost for use by RDS on Outposts.

For Linux, macOS, or Unix:

```
aws rds create-db-subnet-group \
--db-subnet-group-name myoutpostdbsubnetgr \
--db-subnet-group-description "DB subnet group for RDS on Outposts" \
--subnet-ids subnet-abc123
```

For Windows:

```
aws rds create-db-subnet-group ^
--db-subnet-group-name myoutpostdbsubnetgr ^
--db-subnet-group-description "DB subnet group for RDS on Outposts" ^
--subnet-ids subnet-abc123
```

To create an RDS on Outposts DB instance using the AWS CLI

- Use the [create-db-instance](#) command. Specify an Availability Zone for the Outpost, an Amazon VPC security group associated with the Outpost, and the DB subnet group you created for the Outpost. You can include the following options:

- `--db-instance-identifier`
- `--db-instance-class`
- `--engine` – The database engine. Use one of the following values:
 - MySQL – Specify `mysql`.
 - PostgreSQL – Specify `postgres`.
 - Microsoft SQL Server – Specify `sqlserver-ee`, `sqlserver-se`, or `sqlserver-web`.
- `--availability-zone`
- `--vpc-security-group-ids`
- `--db-subnet-group-name`
- `--allocated-storage`
- `--max-allocated-storage`
- `--master-username`
- `--master-user-password`
- `--multi-az` | `--no-multi-az` – (Optional) Whether to create a standby DB instance in a different Availability Zone. The default is `--no-multi-az`.

The `--multi-az` option isn't available for SQL Server.

- `--backup-retention-period`
- `--backup-target` – (Optional) Where to store automated backups and manual snapshots. Use one of the following values:
 - `outposts` – Store them locally on your Outpost.
 - `region` – Store them in the parent AWS Region. This is the default value.

If you use the `--multi-az` option, you can't use `outposts` for `--backup-target`.

- `--storage-encrypted`
- `--kms-key-id`

Example

The following example creates a MySQL DB instance named `myoutpostdbinstance` with backups stored on your Outpost.

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier myoutpostdbinstance \
--engine-version 8.0.17 \
--db-instance-class db.m5.large \
--engine mysql \
--availability-zone us-east-1d \
--vpc-security-group-ids outpost-sg \
--db-subnet-group-name myoutpostdbsubnetgr \
--allocated-storage 100 \
--max-allocated-storage 1000 \
--master-username masterawsuser \
--master-user-password masteruserpassword \
--backup-retention-period 3 \
--backup-target outposts \
--storage-encrypted \
--kms-key-id mykey
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier myoutpostdbinstance ^
--engine-version 8.0.17 ^
--db-instance-class db.m5.large ^
--engine mysql ^
--availability-zone us-east-1d ^
--vpc-security-group-ids outpost-sg ^
--db-subnet-group-name myoutpostdbsubnetgr ^
--allocated-storage 100 ^
--max-allocated-storage 1000 ^
--master-username masterawsuser ^
--master-user-password masteruserpassword ^
--backup-retention-period 3 ^
--backup-target outposts ^
--storage-encrypted ^
--kms-key-id mykey
```

For information about each setting when creating a DB instance, see [Settings for DB instances \(p. 237\)](#).

RDS API

To create a new DB instance in an Outpost with the RDS API, first create a DB subnet group for use by RDS on Outposts by calling the [CreateDBSubnetGroup](#) operation. For SubnetIds, specify the subnet group in the Outpost for use by RDS on Outposts.

Next, call the [CreateDBInstance](#) operation with the following parameters. Specify an Availability Zone for the Outpost, an Amazon VPC security group associated with the Outpost, and the DB subnet group you created for the Outpost.

- `AllocatedStorage`
- `AvailabilityZone`
- `BackupRetentionPeriod`
- `BackupTarget`

- `DBInstanceClass`
- `DBInstanceIdentifier`
- `VpcSecurityGroupIds`
- `DBSubnetGroupName`
- `Engine`
- `EngineVersion`
- `MasterUsername`
- `MasterUserPassword`
- `MaxAllocatedStorage` (optional)
- `MultiAZ` (optional)
- `StorageEncrypted`
- `KmsKeyID`

For information about each setting when creating a DB instance, see [Settings for DB instances \(p. 237\)](#).

Considerations for restoring DB instances on Amazon RDS on AWS Outposts

When you restore a DB instance in Amazon RDS on AWS Outposts, you can generally choose the storage location for automated backups and manual snapshots of the restored DB instance.

- When restoring from a manual DB snapshot, you can store backups either in the parent AWS Region or locally on your Outpost.
- When restoring from an automated backup (point-in-time recovery), you have fewer choices:
 - If restoring from the parent AWS Region, you can store backups either in the AWS Region or on your Outpost.
 - If restoring from your Outpost, you can store backups only on your Outpost.

Using Amazon RDS Proxy

By using Amazon RDS Proxy, you can allow your applications to pool and share database connections to improve their ability to scale. RDS Proxy makes applications more resilient to database failures by automatically connecting to a standby DB instance while preserving application connections. By using RDS Proxy, you can also enforce AWS Identity and Access Management (IAM) authentication for databases, and securely store credentials in AWS Secrets Manager.

Using RDS Proxy, you can handle unpredictable surges in database traffic. Otherwise, these surges might cause issues due to oversubscribing connections or creating new connections at a fast rate. RDS Proxy establishes a database connection pool and reuses connections in this pool. This approach avoids the memory and CPU overhead of opening a new database connection each time. To protect the database against oversubscription, you can control the number of database connections that are created.

RDS Proxy queues or throttles application connections that can't be served immediately from the pool of connections. Although latencies might increase, your application can continue to scale without abruptly failing or overwhelming the database. If connection requests exceed the limits you specify, RDS Proxy rejects application connections (that is, it sheds load). At the same time, it maintains predictable performance for the load that can be served with the available capacity.

You can reduce the overhead to process credentials and establish a secure connection for each new connection. RDS Proxy can handle some of that work on behalf of the database.

RDS Proxy is fully compatible with the engine versions that it supports. You can enable RDS Proxy for most applications with no code changes.

Topics

- [Region and version availability \(p. 921\)](#)
- [Quotas and limitations for RDS Proxy \(p. 921\)](#)
- [Planning where to use RDS Proxy \(p. 924\)](#)
- [RDS Proxy concepts and terminology \(p. 925\)](#)
- [Getting started with RDS Proxy \(p. 929\)](#)
- [Managing an RDS Proxy \(p. 941\)](#)
- [Working with Amazon RDS Proxy endpoints \(p. 952\)](#)
- [Monitoring RDS Proxy metrics with Amazon CloudWatch \(p. 959\)](#)
- [Working with RDS Proxy events \(p. 964\)](#)
- [RDS Proxy command-line examples \(p. 965\)](#)
- [Troubleshooting for RDS Proxy \(p. 967\)](#)
- [Using RDS Proxy with AWS CloudFormation \(p. 972\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of Amazon RDS with RDS Proxy, see [Amazon RDS Proxy \(p. 114\)](#).

Quotas and limitations for RDS Proxy

The following quotas and limitations apply to RDS Proxy:

- You can have up to 20 proxies for each AWS account ID. If your application requires more proxies, you can request additional proxies by opening a ticket with the AWS Support organization.
- Each proxy can have up to 200 associated Secrets Manager secrets. Thus, each proxy can connect to up to 200 different user accounts at any given time.
- You can create, view, modify, and delete up to 20 endpoints for each proxy. These endpoints are in addition to the default endpoint that's automatically created for each proxy.
- In an Aurora cluster, all of the connections using the default proxy endpoint are handled by the Aurora writer instance. To perform load balancing for read-intensive workloads, you can create a read-only endpoint for a proxy. That endpoint passes connections to the reader endpoint of the cluster. That way, your proxy connections can take advantage of Aurora read scalability. For more information, see [Overview of proxy endpoints \(p. 953\)](#).

For RDS DB instances in replication configurations, you can associate a proxy only with the writer DB instance, not a read replica.

- You can use RDS Proxy with Aurora Serverless v2 clusters but not with Aurora Serverless v1 clusters.
- Using RDS Proxy with Aurora clusters that are part of an Aurora global database isn't currently supported.
- Your RDS Proxy must be in the same virtual private cloud (VPC) as the database. The proxy can't be publicly accessible, although the database can be. For example, if you're prototyping on a local host, you can't connect to your RDS Proxy unless you set up dedicated networking. This is the case because your local host is outside of the proxy's VPC.

Note

For Aurora DB clusters, you can turn on cross-VPC access. To do this, create an additional endpoint for a proxy and specify a different VPC, subnets, and security groups with that endpoint. For more information, see [Accessing Aurora and RDS databases across VPCs \(p. 954\)](#).

- You can't use RDS Proxy with a VPC that has its tenancy set to dedicated.
- If you use RDS Proxy with an RDS DB instance or Aurora DB cluster that has IAM authentication enabled, check user authentication. Make sure that all users who connect through a proxy authenticate through user names and passwords. For details about IAM support in RDS Proxy, see [Setting up AWS Identity and Access Management \(IAM\) policies \(p. 932\)](#).
- You can't use RDS Proxy with custom DNS.
- Each proxy can be associated with a single target DB instance or cluster. However, you can associate multiple proxies with the same DB instance or cluster.
- Any statement with a text size greater than 16 KB causes the proxy to pin the session to the current connection.

For additional limitations for each DB engine, see the following sections:

- [Additional limitations for RDS for MariaDB \(p. 922\)](#)
- [Additional limitations for RDS for Microsoft SQL Server \(p. 923\)](#)
- [Additional limitations for RDS for MySQL \(p. 923\)](#)
- [Additional limitations for RDS for PostgreSQL \(p. 924\)](#)

Additional limitations for RDS for MariaDB

The following additional limitations apply to RDS Proxy with RDS for MariaDB databases:

- Currently, all proxies listen on port 3306 for MariaDB. The proxies still connect to your database using the port that you specified in the database settings.

- You can't use RDS Proxy with self-managed MariaDB databases in Amazon EC2 instances.
- You can't use RDS Proxy with an RDS for MariaDB DB instance that has the `read_only` parameter in its DB parameter group set to 1.
- RDS Proxy doesn't support compressed mode. For example, it doesn't support the compression used by the `--compress` or `-C` options of the `mysql` command.
- Some SQL statements and functions can change the connection state without causing pinning. For the most current pinning behavior, see [Avoiding pinning \(p. 948\)](#).
- RDS Proxy doesn't support the MariaDB `auth_ed25519` plugin.
- RDS Proxy doesn't support Transport Layer Security (TLS) version 1.3 for MariaDB databases.

Important

For proxies associated with MariaDB databases, don't set the configuration parameter `sql_auto_is_null` to `true` or a nonzero value in the initialization query. Doing so might cause incorrect application behavior.

Additional limitations for RDS for Microsoft SQL Server

The following additional limitations apply to RDS Proxy with RDS for Microsoft SQL Server databases:

- The number of Secrets Manager secrets that you need to create for a proxy depends on the collation that your DB instance uses. For example, suppose that your DB instance uses case-sensitive collation. If your application accepts both "Admin" and "admin," then your proxy needs two separate secrets. For more information about collation in SQL Server, see the [Microsoft SQL Server](#) documentation.
- RDS Proxy doesn't support connections that use Active Directory.
- You can't use IAM authentication with clients that don't support token properties. For more information, see [Considerations for connecting to a proxy with Microsoft SQL Server \(p. 940\)](#).
- The results of `@@IDENTITY`, `@@ROWCOUNT`, and `SCOPE_IDENTITY` aren't always accurate. As a work-around, retrieve their values in the same session statement to ensure that they return the correct information.
- If the connection uses multiple active result sets (MARS), RDS Proxy doesn't run the initialization queries. For information about MARS, see the [Microsoft SQL Server](#) documentation.

Additional limitations for RDS for MySQL

The following additional limitations apply to RDS Proxy with RDS for MySQL databases:

- RDS Proxy doesn't support the MySQL `sha256_password` and `caching_sha2_password` authentication plugins. These plugins implement SHA-256 hashing for user account passwords.
- Currently, all proxies listen on port 3306 for MySQL. The proxies still connect to your database using the port that you specified in the database settings.
- You can't use RDS Proxy with self-managed MySQL databases in EC2 instances.
- You can't use RDS Proxy with an RDS for MySQL DB instance that has the `read_only` parameter in its DB parameter group set to 1.
- RDS Proxy doesn't support MySQL compressed mode. For example, it doesn't support the compression used by the `--compress` or `-C` options of the `mysql` command.
- Some SQL statements and functions can change the connection state without causing pinning. For the most current pinning behavior, see [Avoiding pinning \(p. 948\)](#).

Important

For proxies associated with MySQL databases, don't set the configuration parameter `sql_auto_is_null` to true or a nonzero value in the initialization query. Doing so might cause incorrect application behavior.

Additional limitations for RDS for PostgreSQL

The following additional limitations apply to RDS Proxy with RDS for PostgreSQL databases:

- RDS Proxy doesn't support session pinning filters for PostgreSQL.
- RDS Proxy doesn't support PostgreSQL SCRAM-SHA-256 authentication.
- Currently, all proxies listen on port 5432 for PostgreSQL.
- For PostgreSQL, RDS Proxy doesn't currently support canceling a query from a client by issuing a `CancelRequest`. This is the case, for example, when you cancel a long-running query in an interactive `psql` session by using `Ctrl+C`.
- The results of the PostgreSQL function `lastval` aren't always accurate. As a work-around, use the `INSERT` statement with the `RETURNING` clause.
- RDS Proxy doesn't multiplex connections when your client application drivers use the PostgreSQL extended query protocol.
- RDS Proxy currently doesn't support streaming replication mode.

Planning where to use RDS Proxy

You can determine which of your DB instances, clusters, and applications might benefit the most from using RDS Proxy. To do so, consider these factors:

- Any DB instance or cluster that encounters "too many connections" errors is a good candidate for associating with a proxy. The proxy enables applications to open many client connections, while the proxy manages a smaller number of long-lived connections to the DB instance or cluster.
- For DB instances or clusters that use smaller AWS instance classes, such as T2 or T3, using a proxy can help avoid out-of-memory conditions. It can also help reduce the CPU overhead for establishing connections. These conditions can occur when dealing with large numbers of connections.
- You can monitor certain Amazon CloudWatch metrics to determine whether a DB instance or cluster is approaching certain types of limit. These limits are for the number of connections and the memory associated with connection management. You can also monitor certain CloudWatch metrics to determine whether a DB instance or cluster is handling many short-lived connections. Opening and closing such connections can impose performance overhead on your database. For information about the metrics to monitor, see [Monitoring RDS Proxy metrics with Amazon CloudWatch \(p. 959\)](#).
- AWS Lambda functions can also be good candidates for using a proxy. These functions make frequent short database connections that benefit from connection pooling offered by RDS Proxy. You can take advantage of any IAM authentication you already have for Lambda functions, instead of managing database credentials in your Lambda application code.
- Applications that typically open and close large numbers of database connections and don't have built-in connection pooling mechanisms are good candidates for using a proxy.
- Applications that keep a large number of connections open for long periods are typically good candidates for using a proxy. Applications in industries such as software as a service (SaaS) or ecommerce often minimize the latency for database requests by leaving connections open. With RDS Proxy, an application can keep more connections open than it can when connecting directly to the DB instance or cluster.
- You might not have adopted IAM authentication and Secrets Manager due to the complexity of setting up such authentication for all DB instances and clusters. If so, you can leave the existing authentication methods in place and delegate the authentication to a proxy. The proxy can enforce

the authentication policies for client connections for particular applications. You can take advantage of any IAM authentication you already have for Lambda functions, instead of managing database credentials in your Lambda application code.

- RDS Proxy can help make applications more resilient and transparent to database failures. RDS Proxy bypasses Domain Name System (DNS) caches to reduce failover times by up to 66% for Amazon RDS Multi-AZ databases. RDS Proxy also automatically routes traffic to a new database instance while preserving application connections. This makes failovers more transparent for applications.

RDS Proxy concepts and terminology

You can simplify connection management for your Amazon RDS DB instances and Amazon Aurora DB clusters by using RDS Proxy.

RDS Proxy handles the network traffic between the client application and the database. It does so in an active way first by understanding the database protocol. It then adjusts its behavior based on the SQL operations from your application and the result sets from the database.

RDS Proxy reduces the memory and CPU overhead for connection management on your database. The database needs less memory and CPU resources when applications open many simultaneous connections. It also doesn't require logic in your applications to close and reopen connections that stay idle for a long time. Similarly, it requires less application logic to reestablish connections in case of a database problem.

The infrastructure for RDS Proxy is highly available and deployed over multiple Availability Zones (AZs). The computation, memory, and storage for RDS Proxy are independent of your RDS DB instances and Aurora DB clusters. This separation helps lower overhead on your database servers, so that they can devote their resources to serving database workloads. The RDS Proxy compute resources are serverless, automatically scaling based on your database workload.

Topics

- [Overview of RDS Proxy concepts \(p. 925\)](#)
- [Connection pooling \(p. 926\)](#)
- [RDS Proxy security \(p. 926\)](#)
- [Failover \(p. 928\)](#)
- [Transactions \(p. 928\)](#)

Overview of RDS Proxy concepts

RDS Proxy handles the infrastructure to perform connection pooling and the other features described in the sections that follow. You see the proxies represented in the RDS console on the [Proxies](#) page.

Each proxy handles connections to a single RDS DB instance or Aurora DB cluster. The proxy automatically determines the current writer instance for RDS Multi-AZ DB instances and Aurora provisioned clusters. For Aurora multi-master clusters, the proxy connects to one of the writer instances and uses the other writer instances as hot standby targets.

The connections that a proxy keeps open and available for your database application to use make up the *connection pool*.

By default, RDS Proxy can reuse a connection after each transaction in your session. This transaction-level reuse is called *multiplexing*. When RDS Proxy temporarily removes a connection from the connection pool to reuse it, that operation is called *borrowing* the connection. When it's safe to do so, RDS Proxy returns that connection to the connection pool.

In some cases, RDS Proxy can't be sure that it's safe to reuse a database connection outside of the current session. In these cases, it keeps the session on the same connection until the session ends. This fallback behavior is called *pinning*.

A proxy has a default endpoint. You connect to this endpoint when you work with an RDS DB instance or Aurora DB cluster. You do so instead of connecting to the read/write endpoint that connects directly to the instance or cluster. The special-purpose endpoints for an Aurora cluster remain available for you to use. For Aurora DB clusters, you can also create additional read/write and read-only endpoints. For more information, see [Overview of proxy endpoints \(p. 953\)](#).

For example, you can still connect to the cluster endpoint for read/write connections without connection pooling. You can still connect to the reader endpoint for load-balanced read-only connections. You can still connect to the instance endpoints for diagnosis and troubleshooting of specific DB instances within an Aurora cluster. If you use other AWS services such as AWS Lambda to connect to RDS databases, change their connection settings to use the proxy endpoint. For example, you specify the proxy endpoint to allow Lambda functions to access your database while taking advantage of RDS Proxy functionality.

Each proxy contains a target group. This *target group* embodies the RDS DB instance or Aurora DB cluster that the proxy can connect to. For an Aurora cluster, by default the target group is associated with all the DB instances in that cluster. That way, the proxy can connect to whichever Aurora DB instance is promoted to be the writer instance in the cluster. The RDS DB instance associated with a proxy, or the Aurora DB cluster and its instances, are called the *targets* of that proxy. For convenience, when you create a proxy through the console, RDS Proxy also creates the corresponding target group and registers the associated targets automatically.

An *engine family* is a related set of database engines that use the same DB protocol. You choose the engine family for each proxy that you create.

Connection pooling

Each proxy performs connection pooling for the writer instance of its associated RDS or Aurora database. *Connection pooling* is an optimization that reduces the overhead associated with opening and closing connections and with keeping many connections open simultaneously. This overhead includes memory needed to handle each new connection. It also involves CPU overhead to close each connection and open a new one. Examples include Transport Layer Security/Secure Sockets Layer (TLS/SSL) handshaking, authentication, negotiating capabilities, and so on. Connection pooling simplifies your application logic. You don't need to write application code to minimize the number of simultaneous open connections.

Each proxy also performs connection multiplexing, also known as connection reuse. With *multiplexing*, RDS Proxy performs all the operations for a transaction using one underlying database connection. RDS then can use a different connection for the next transaction. You can open many simultaneous connections to the proxy, and the proxy keeps a smaller number of connections open to the DB instance or cluster. Doing so further minimizes the memory overhead for connections on the database server. This technique also reduces the chance of "too many connections" errors.

RDS Proxy security

RDS Proxy uses the existing RDS security mechanisms such as TLS/SSL and AWS Identity and Access Management (IAM). For general information about those security features, see [Security in Amazon RDS \(p. 1997\)](#). Also, make sure to familiarize yourself with how RDS and Aurora work with authentication, authorization, and other areas of security.

RDS Proxy can act as an additional layer of security between client applications and the underlying database. For example, you can connect to the proxy using TLS 1.2, even if the underlying DB instance supports only TLS 1.0 or 1.1. You can connect to the proxy using an IAM role. This is so even if the proxy connects to the database using the native user and password authentication method. By using this technique, you can enforce strong authentication requirements for database applications without a costly migration effort for the DB instances themselves.

You store the database credentials used by RDS Proxy in AWS Secrets Manager. Each database user for the RDS DB instance or Aurora DB cluster accessed by a proxy must have a corresponding secret in Secrets Manager. You can also set up IAM authentication for users of RDS Proxy. By doing so, you can enforce IAM authentication for database access even if the databases use native password authentication. We recommend using these security features instead of embedding database credentials in your application code.

Using TLS/SSL with RDS Proxy

You can connect to RDS Proxy using the TLS/SSL protocol.

Note

RDS Proxy uses certificates from the AWS Certificate Manager (ACM). If you use RDS Proxy, when you rotate your TLS/SSL certificate you don't need to update applications that use RDS Proxy connections.

To enforce TLS for all connections between the proxy and your database, you can specify a setting **Require Transport Layer Security** when you create or modify a proxy.

RDS Proxy can also ensure that your session uses TLS/SSL between your client and the RDS Proxy endpoint. To have RDS Proxy do so, specify the requirement on the client side. SSL session variables are not set for SSL connections to a database using RDS Proxy.

- For RDS for MySQL and Aurora MySQL, specify the requirement on the client side with the `--ssl-` mode parameter when you run the `mysql` command.
- For Amazon RDS PostgreSQL and Aurora PostgreSQL, specify `sslmode=require` as part of the `conninfo` string when you run the `psql` command.

RDS Proxy supports TLS protocol version 1.0, 1.1, and 1.2. You can connect to the proxy using a higher version of TLS than you use in the underlying database.

By default, client programs establish an encrypted connection with RDS Proxy, with further control available through the `--ssl-mode` option. From the client side, RDS Proxy supports all SSL modes.

For the client, the SSL modes are the following:

PREFERRED

SSL is the first choice, but it isn't required.

DISABLED

No SSL is allowed.

REQUIRED

Enforce SSL.

VERIFY_CA

Enforce SSL and verify the certificate authority (CA).

VERIFY_IDENTITY

Enforce SSL and verify the CA and CA hostname.

When using a client with `--ssl-mode VERIFY_CA` or `VERIFY_IDENTITY`, specify the `--ssl-ca` option pointing to a CA in .pem format. For the .pem file to use, download all root CA PEMs from [Amazon Trust Services](#) and place them into a single .pem file.

RDS Proxy uses wildcard certificates, which apply to both a domain and its subdomains. If you use the `mysql` client to connect with SSL mode `VERIFY_IDENTITY`, currently you must use the MySQL 8.0-compatible `mysql` command.

Failover

Failover is a high-availability feature that replaces a database instance with another one when the original instance becomes unavailable. A failover might happen because of a problem with a database instance. It might also be part of normal maintenance procedures, such as during a database upgrade. Failover applies to RDS DB instances in a Multi-AZ configuration. Failover applies to Aurora DB clusters with one or more reader instances in addition to the writer instance.

Connecting through a proxy makes your application more resilient to database failovers. When the original DB instance becomes unavailable, RDS Proxy connects to the standby database without dropping idle application connections. Doing so helps to speed up and simplify the failover process. The result is faster failover that's less disruptive to your application than a typical reboot or database problem.

Without RDS Proxy, a failover involves a brief outage. During the outage, you can't perform write operations on that database. Any existing database connections are disrupted, and your application must reopen them. The database becomes available for new connections and write operations when a read-only DB instance is promoted in place of one that's unavailable.

During DB failovers, RDS Proxy continues to accept connections at the same IP address and automatically directs connections to the new primary DB instance. Clients connecting through RDS Proxy are not susceptible to the following:

- Domain Name System (DNS) propagation delays on failover.
- Local DNS caching.
- Connection timeouts.
- Uncertainty about which DB instance is the current writer.
- Waiting for a query response from a former writer that became unavailable without closing connections.

For applications that maintain their own connection pool, going through RDS Proxy means that most connections stay alive during failovers or other disruptions. Only connections that are in the middle of a transaction or SQL statement are canceled. RDS Proxy immediately accepts new connections. When the database writer is unavailable, RDS Proxy queues up incoming requests.

For applications that don't maintain their own connection pools, RDS Proxy offers faster connection rates and more open connections. It offloads the expensive overhead of frequent reconnects from the database. It does so by reusing database connections maintained in the RDS Proxy connection pool. This approach is particularly important for TLS connections, where setup costs are significant.

Transactions

All the statements within a single transaction always use the same underlying database connection. The connection becomes available for use by a different session when the transaction ends. Using the transaction as the unit of granularity has the following consequences:

- Connection reuse can happen after each individual statement when the RDS for MySQL or Aurora MySQL `autocommit` setting is turned on.
- Conversely, when the `autocommit` setting is turned off, the first statement you issue in a session begins a new transaction. For example, suppose that you enter a sequence of `SELECT`, `INSERT`, `UPDATE`, and other data manipulation language (DML) statements. In this case, connection reuse doesn't happen until you issue a `COMMIT`, `ROLLBACK`, or otherwise end the transaction.
- Entering a data definition language (DDL) statement causes the transaction to end after that statement completes.

RDS Proxy detects when a transaction ends through the network protocol used by the database client application. Transaction detection doesn't rely on keywords such as COMMIT or ROLLBACK appearing in the text of the SQL statement.

In some cases, RDS Proxy might detect a database request that makes it impractical to move your session to a different connection. In these cases, it turns off multiplexing for that connection the remainder of your session. The same rule applies if RDS Proxy can't be certain that multiplexing is practical for the session. This operation is called *pinning*. For ways to detect and minimize pinning, see [Avoiding pinning \(p. 948\)](#).

Getting started with RDS Proxy

In the following sections, you can find how to set up RDS Proxy. You can also find how to set related security options. These control who can access each proxy and how each proxy connects to DB instances.

Topics

- [Setting up network prerequisites \(p. 929\)](#)
- [Setting up database credentials in AWS Secrets Manager \(p. 931\)](#)
- [Setting up AWS Identity and Access Management \(IAM\) policies \(p. 932\)](#)
- [Creating an RDS Proxy \(p. 934\)](#)
- [Viewing an RDS Proxy \(p. 938\)](#)
- [Connecting to a database through RDS Proxy \(p. 939\)](#)

Setting up network prerequisites

Using RDS Proxy requires you to have a common virtual private cloud (VPC) between your Aurora DB cluster or RDS DB instance and RDS Proxy. This VPC should have a minimum of two subnets that are in different Availability Zones. Your account can either own these subnets or share them with other accounts. For information about VPC sharing, see [Work with shared VPCs](#). Your client application resources such as Amazon EC2, Lambda, or Amazon ECS can be in the same VPC as the proxy. Or they can be in a separate VPC from the proxy. If you successfully connected to any RDS DB instances or Aurora DB clusters, you already have the required network resources.

Topics

- [Getting information about your subnets \(p. 929\)](#)
- [Planning for IP address capacity \(p. 930\)](#)

Getting information about your subnets

The following Linux example shows AWS CLI commands that examine the VPCs and subnets owned by your AWS account. In particular, you pass subnet IDs as parameters when you create a proxy using the CLI.

```
aws ec2 describe-vpcs
aws ec2 describe-internet-gateways
aws ec2 describe-subnets --query '*[].[VpcId,SubnetId]' --output text | sort
```

The following Linux example shows AWS CLI commands to determine the subnet IDs corresponding to a specific Aurora DB cluster or RDS DB instance. For an Aurora cluster, first you find the ID for one of the associated DB instances. You can extract the subnet IDs used by that DB instance. To do so, examine the nested fields within the DBSubnetGroup and Subnets attributes in the describe output for the DB instance. You specify some or all of those subnet IDs when setting up a proxy for that database server.

```
$ # Optional first step, only needed if you're starting from an Aurora cluster. Find the ID
of any DB instance in the cluster.
$ aws rds describe-db-clusters --db-cluster-identifier my_cluster_id --query '*[]'.
[DBClusterMembers][0][0][*].DBInstanceIdentifier' --output text
my_instance_id
instance_id_2
instance_id_3
...
$ # From the DB instance, trace through the DBSubnetGroup and Subnets to find the subnet
IDs.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[]'.
[DBSubnetGroup][0][0][Subnets][0][*].SubnetIdentifier' --output text
subnet_id_1
subnet_id_2
subnet_id_3
...
```

Or you can first find the VPC ID for the DB instance. Then you can examine the VPC to find its subnets. The following Linux example shows how.

```
$ # From the DB instance, find the VPC.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[]'.
[DBSubnetGroup][0][0].VpcId' --output text
my_vpc_id

$ aws ec2 describe-subnets --filters Name=vpc-id,Values=my_vpc_id --query '*[].[SubnetId]'
--output text
subnet_id_1
subnet_id_2
subnet_id_3
subnet_id_4
subnet_id_5
subnet_id_6
```

Planning for IP address capacity

An RDS Proxy automatically adjusts its capacity as needed based on the size and number of DB instances registered with it. Certain operations might also require additional proxy capacity. Some examples are increasing the size of a registered database or internal RDS Proxy maintenance operations. During these operations, your proxy might need more IP addresses to provision the extra capacity. These additional addresses allow your proxy to scale without affecting your workload. A lack of free IP addresses in your subnets prevents a proxy from scaling up. This can lead to higher query latencies or client connection failures. RDS notifies you through event RDS-EVENT-0243 when there aren't enough free IP addresses in your subnets. For information about this event, see [Working with RDS Proxy events \(p. 964\)](#).

Following are the recommended minimum number of IP addresses to leave free in your subnets for your proxy based on DB instance class sizes.

DB instance class	Minimum free IP addresses
db.*.xlarge or smaller	10
db.*.2xlarge	15
db.*.4xlarge	25
db.*.8xlarge	45

DB instance class	Minimum free IP addresses
db.*.12xlarge	60
db.*.16xlarge	75
db.*.24xlarge	110

These numbers of recommended IP addresses are estimates for a proxy with only the default endpoint. A proxy with additional endpoints or read replicas might need more free IP addresses. For each additional endpoint, we recommend that you reserve three more IP addresses. For each read replica, we recommend that you reserve additional IP addresses as specified in the table based on that read replica's size.

Note

RDS Proxy never uses more than 215 IP addresses in a VPC.

Setting up database credentials in AWS Secrets Manager

For each proxy that you create, you first use the Secrets Manager service to store sets of user name and password credentials. You create a separate Secrets Manager secret for each database user account that the proxy connects to on the RDS DB instance or Aurora DB cluster.

In Secrets Manager, you create these secrets with values for the **username** and **password** fields. Doing so allows the proxy to connect to the corresponding database users on RDS DB instances or Aurora DB clusters that you associate with the proxy. To do this, you can use the setting **Credentials for other database**, **Credentials for RDS database**, or **Other type of secrets**. Fill in the appropriate values for the **User name** and **Password** fields, and placeholder values for any other required fields. The proxy ignores other fields such as **Host** and **Port** if they're present in the secret. Those details are automatically supplied by the proxy.

You can also choose **Other type of secrets**. In this case, you create the secret with keys named **username** and **password**.

Because the secrets used by your proxy aren't tied to a specific database server, you can reuse a secret across multiple proxies. To do so, use the same credentials across multiple database servers. For example, you might use the same credentials across a group of development and test servers.

To connect through the proxy as a specific user, make sure that the password associated with a secret matches the database password for that user. If there's a mismatch, you can update the associated secret in Secrets Manager. In this case, you can still connect to other accounts where the secret credentials and the database passwords do match.

Note

For RDS for SQL Server, the number of Secrets Manager secrets that you need to create for a proxy depends on the collation that your DB instance uses. For example, suppose that your DB instance uses case-sensitive collation. If your application accepts both "Admin" and "admin," then your proxy needs two separate secrets. For more information about collation in SQL Server, see the [Microsoft SQL Server](#) documentation.

When you create a proxy through the AWS CLI or RDS API, you specify the Amazon Resource Names (ARNs) of the corresponding secrets. You do so for all the DB user accounts that the proxy can access. In the AWS Management Console, you choose the secrets by their descriptive names.

For instructions about creating secrets in Secrets Manager, see the [Creating a secret](#) page in the Secrets Manager documentation. Use one of the following techniques:

- Use [Secrets Manager](#) in the console.
- To use the CLI to create a Secrets Manager secret for use with RDS Proxy, use a command such as the following.

```
aws secretsmanager create-secret \
--name "secret_name"
--description "secret_description"
--region region_name
--secret-string '{"username":"db_user","password":"db_user_password"}'
```

For example, the following commands create Secrets Manager secrets for two database users, one named admin and the other named app-user.

```
aws secretsmanager create-secret \
--name admin_secret_name --description "db admin user" \
--secret-string '{"username":"admin","password":"choose_your_own_password"}'

aws secretsmanager create-secret \
--name proxy_secret_name --description "application user" \
--secret-string '{"username":"app-user","password":"choose_your_own_password"}'
```

To see the secrets owned by your AWS account, use a command such as the following.

```
aws secretsmanager list-secrets
```

When you create a proxy using the CLI, you pass the Amazon Resource Names (ARNs) of one or more secrets to the --auth parameter. The following Linux example shows how to prepare a report with only the name and ARN of each secret owned by your AWS account. This example uses the --output table parameter that is available in AWS CLI version 2. If you are using AWS CLI version 1, use --output text instead.

```
aws secretsmanager list-secrets --query '*[].[Name,ARN]' --output table
```

To verify that you stored the correct credentials and in the right format in a secret, use a command such as the following. Substitute the short name or the ARN of the secret for [your_secret_name](#).

```
aws secretsmanager get-secret-value --secret-id your_secret_name
```

The output should include a line displaying a JSON-encoded value like the following.

```
"SecretString": "{\"username\":\"your_username\",\"password\":\"your_password\"}",
```

Setting up AWS Identity and Access Management (IAM) policies

After you create the secrets in Secrets Manager, you create an IAM policy that can access those secrets. For general information about using IAM with RDS and Aurora, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

Tip

The following procedure applies if you use the IAM console. If you use the AWS Management Console for RDS, RDS can create the IAM policy for you automatically. In that case, you can skip the following procedure.

To create an IAM policy that accesses your Secrets Manager secrets for use with your proxy

1. Sign in to the IAM console. Follow the [Create role](#) process, as described in [Creating IAM roles](#). Include the **Add Role to Database** step.
2. For the new role, perform the **Add inline policy** step. Use the same general procedures as in [Editing IAM policies](#). Paste the following JSON into the JSON text box. Substitute your own account ID. Substitute your AWS Region for us-east-2. Substitute the Amazon Resource Names (ARNs) for the secrets that you created. For the kms :Decrypt action, substitute the ARN of the default AWS KMS key or your own KMS key. Which one you use depends on which one you used to encrypt the Secrets Manager secrets.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_1",
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_2"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-2:account_id:key/key_id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

3. Edit the trust policy for this IAM role. Paste the following JSON into the JSON text box.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

The following commands perform the same operation through the AWS CLI.

```
PREFIX=choose_an_identifier
aws iam create-role --role-name choose_role_name \
--assume-role-policy-document '{"Version":"2012-10-17","Statement": [{"Effect":"Allow","Principal":{"Service": ["rds.amazonaws.com"]}}, {"Action": "sts:AssumeRole"}]}'
```

```

aws iam put-role-policy --role-name same_role_name_as_previous \
--policy-name $PREFIX-secret-reader-policy --policy-document """
same_json_as_in_previous_example
"""

aws kms create-key --description "$PREFIX-test-key" --policy """
{
  "Id": "$PREFIX-kms-policy",
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::account_id:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal":
      {
        "AWS":
          ["$USER_ARN", "arn:aws:iam::account_id:role/Admin"]
      },
      "Action":
      [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms>List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms>Delete*",
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ScheduleKeyDeletion",
        "kms:CancelKeyDeletion"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {"AWS": "$ROLE_ARN"},
      "Action": ["kms:Decrypt", "kms:DescribeKey"],
      "Resource": "*"
    }
  ]
}
"""

```

Creating an RDS Proxy

To manage connections for a specified set of DB instances, you can create a proxy. You can associate a proxy with an RDS for MariaDB, RDS for Microsoft SQL Server, RDS for MySQL, or RDS for PostgreSQL DB instance.

AWS Management Console

To create a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. Choose **Create proxy**.
4. Choose all the settings for your proxy.

For **Proxy configuration**, provide information for the following:

- **Proxy identifier.** Specify a name of your choosing, unique within your AWS account ID and current AWS Region.
- **Engine family.** This setting determines which database network protocol the proxy recognizes when it interprets network traffic to and from the database. For RDS for MariaDB or RDS for MySQL, choose **MySQL**. For RDS for PostgreSQL, choose **PostgreSQL**. For RDS for SQL Server, choose **SQL Server**.
- **Require Transport Layer Security.** Choose this setting if you want the proxy to enforce TLS/SSL for all client connections. For an encrypted or unencrypted connection to a proxy, the proxy uses the same encryption setting when it makes a connection to the underlying database.
- **Idle client connection timeout.** Choose a time period that a client connection can be idle before the proxy can close it. The default is 1,800 seconds (30 minutes). A client connection is considered idle when the application doesn't submit a new request within the specified time after the previous request completed. The underlying database connection stays open and is returned to the connection pool. Thus, it's available to be reused for new client connections.

Consider lowering the idle client connection timeout if you want the proxy to proactively remove stale connections. If your workload is spiking, consider raising the idle client connection timeout to save the cost of establishing connections.

For **Target group configuration**, provide information for the following:

- **Database.** Choose one RDS DB instance or Aurora DB cluster to access through this proxy. The list only includes DB instances and clusters with compatible database engines, engine versions, and other settings. If the list is empty, create a new DB instance or cluster that's compatible with RDS Proxy. To do so, follow the procedure in [Creating an Amazon RDS DB instance \(p. 230\)](#). Then try creating the proxy again.
- **Connection pool maximum connections.** Specify a value from 1 through 100. This setting represents the percentage of the `max_connections` value that RDS Proxy can use for its connections. If you only intend to use one proxy with this DB instance or cluster, you can set this value to 100. For details about how RDS Proxy uses this setting, see [MaxConnectionsPercent \(p. 947\)](#).
- **Session pinning filters.** (Optional) This is an advanced setting, for troubleshooting performance issues with particular applications. Currently, the setting isn't supported for PostgreSQL and the only choice is `EXCLUDE_VARIABLE_SETS`. Choose a filter only if both of following are true: First, your application isn't reusing connections due to certain kinds of SQL statements. Also, you can verify that reusing connections with those SQL statements doesn't affect application correctness. For more information, see [Avoiding pinning \(p. 948\)](#).
- **Connection borrow timeout.** In some cases, you might expect the proxy to sometimes use all available database connections. In such cases, you can specify how long the proxy waits for a database connection to become available before returning a timeout error. You can specify a period up to a maximum of five minutes. This setting only applies when the proxy has the maximum number of connections open and all connections are already in use.

- **Initialization query.** (Optional) You can specify one or more SQL statements for the proxy to run when opening each new database connection. The setting is typically used with SET statements to make sure that each connection has identical settings such as time zone and character set. For multiple statements, use semicolons as the separator. You can also include multiple variables in a single SET statement, such as SET x=1, y=2. Initialization query is not currently supported for PostgreSQL.

For **Connectivity**, provide information for the following:

- **Secrets Manager secrets.** Choose at least one Secrets Manager secret that contains database user credentials for the RDS DB instance or Aurora DB cluster to access with this proxy.
- **IAM role.** Choose an IAM role that has permission to access the Secrets Manager secrets that you chose earlier. You can also choose for the AWS Management Console to create a new IAM role for you and use that.
- **IAM Authentication.** Choose whether to require, allow, or disallow IAM authentication for connections to your proxy. The allow option is only valid for proxies for RDS for SQL Server. The choice of IAM authentication or native database authentication applies to all DB users that access this proxy.
- **Subnets.** This field is prepopulated with all the subnets associated with your VPC. You can remove any subnets that you don't need for this proxy. You must leave at least two subnets.

Provide additional connectivity configuration:

- **VPC security group.** Choose an existing VPC security group. You can also choose for the AWS Management Console to create a new security group for you and use that.

Note

This security group must allow access to the database the proxy connects to. The same security group is used for ingress from your applications to the proxy, and for egress from the proxy to the database. For example, suppose that you use the same security group for your database and your proxy. In this case, make sure that you specify that resources in that security group can communicate with other resources in the same security group. When using a shared VPC, you can't use the default security group for the VPC, or one that belongs to another account. Choose a security group that belongs to your account. If one doesn't exist, create one. For more information about this limitation, see [Work with shared VPCs](#).

(Optional) Provide advanced configuration:

- **Enable enhanced logging.** You can enable this setting to troubleshoot proxy compatibility or performance issues.

When this setting is enabled, RDS Proxy includes detailed information about SQL statements in its logs. This information helps you to debug issues involving SQL behavior or the performance and scalability of the proxy connections. The debug information includes the text of SQL statements that you submit through the proxy. Thus, only enable this setting when needed for debugging. Also, only enable it when you have security measures in place to safeguard any sensitive information that appears in the logs.

To minimize overhead associated with your proxy, RDS Proxy automatically turns this setting off 24 hours after you enable it. Enable it temporarily to troubleshoot a specific issue.

5. Choose **Create Proxy**.

AWS CLI

To create a proxy, use the AWS CLI command [create-db-proxy](#). The `--engine-family` value is case-sensitive.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-proxy \
--db-proxy-name proxy_name \
--engine-family { MYSQL | POSTGRESQL | SQLSERVER } \
--auth ProxyAuthenticationConfig_JSON_string \
--role-arn iam_role \
--vpc-subnet-ids space_separated_list \
[--vpc-security-group-ids space_separated_list] \
[--require-tls | --no-require-tls] \
[--idle-client-timeout value] \
[--debug-logging | --no-debug-logging] \
[--tags comma_separated_list]
```

For Windows:

```
aws rds create-db-proxy ^
--db-proxy-name proxy_name ^
--engine-family { MYSQL | POSTGRESQL | SQLSERVER } ^
--auth ProxyAuthenticationConfig_JSON_string ^
--role-arn iam_role ^
--vpc-subnet-ids space_separated_list ^
[--vpc-security-group-ids space_separated_list] ^
[--require-tls | --no-require-tls] ^
[--idle-client-timeout value] ^
[--debug-logging | --no-debug-logging] ^
[--tags comma_separated_list]
```

Tip

If you don't already know the subnet IDs to use for the `--vpc-subnet-ids` parameter, see [Setting up network prerequisites \(p. 929\)](#) for examples of how to find them.

Note

The security group must allow access to the database the proxy connects to. The same security group is used for ingress from your applications to the proxy, and for egress from the proxy to the database. For example, suppose that you use the same security group for your database and your proxy. In this case, make sure that you specify that resources in that security group can communicate with other resources in the same security group.

When using a shared VPC, you can't use the default security group for the VPC, or one that belongs to another account. Choose a security group that belongs to your account. If one doesn't exist, create one. For more information about this limitation, see [Work with shared VPCs](#).

To create the required information and associations for the proxy, you also use the [register-db-proxy-targets](#) command. Specify the target group name `default`. RDS Proxy automatically creates a target group with this name when you create each proxy.

```
aws rds register-db-proxy-targets
--db-proxy-name value
[--target-group-name target_group_name]
[--db-instance-identifiers space_separated_list] # rds db instances, or
[--db-cluster-identifiers cluster_id]           # rds db cluster (all instances), or
[--db-cluster-endpoint endpoint_name]          # rds db cluster endpoint (all
instances)
```

RDS API

To create an RDS proxy, call the Amazon RDS API operation [CreateDBProxy](#). You pass a parameter with the [AuthConfig](#) data structure.

RDS Proxy automatically creates a target group named `default` when you create each proxy. You associate an RDS DB instance or Aurora DB cluster with the target group by calling the function [RegisterDBProxyTargets](#).

Viewing an RDS Proxy

After you create one or more RDS proxies, you can view them all. Doing so makes it possible to examine their configuration details and choose which ones to modify, delete, and so on.

Any database applications that use the proxy require the proxy endpoint to use in the connection string.

AWS Management Console

To view your proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region in which you created the RDS Proxy.
3. In the navigation pane, choose **Proxies**.
4. Choose the name of an RDS proxy to display its details.
5. On the details page, the **Target groups** section shows how the proxy is associated with a specific RDS DB instance or Aurora DB cluster. You can follow the link to the **default** target group page to see more details about the association between the proxy and the database. This page is where you see settings that you specified when creating the proxy. These include maximum connection percentage, connection borrow timeout, engine family, and session pinning filters.

CLI

To view your proxy using the CLI, use the `describe-db-proxies` command. By default, it displays all proxies owned by your AWS account. To see details for a single proxy, specify its name with the `--db-proxy-name` parameter.

```
aws rds describe-db-proxies [--db-proxy-name proxy_name]
```

To view the other information associated with the proxy, use the following commands.

```
aws rds describe-db-proxy-target-groups --db-proxy-name proxy_name  
aws rds describe-db-proxy-targets --db-proxy-name proxy_name
```

Use the following sequence of commands to see more detail about the things that are associated with the proxy:

1. To get a list of proxies, run `describe-db-proxies`.
2. To show connection parameters such as the maximum percentage of connections that the proxy can use, run `describe-db-proxy-target-groups` `--db-proxy-name`. Use the name of the proxy as the parameter value.
3. To see the details of the RDS DB instance or Aurora DB cluster associated with the returned target group, run `describe-db-proxy-targets`.

RDS API

To view your proxies using the RDS API, use the [DescribeDBProxies](#) operation. It returns values of the [DBProxy](#) data type.

To see details of the connection settings for the proxy, use the proxy identifiers from this return value with the [DescribeDBProxyTargetGroups](#) operation. It returns values of the [DBProxyTargetGroup](#) data type.

To see the RDS instance or Aurora DB cluster associated with the proxy, use the [DescribeDBProxyTargets](#) operation. It returns values of the [DBProxyTarget](#) data type.

Connecting to a database through RDS Proxy

You connect to an RDS DB instance or Aurora DB cluster through a proxy in generally the same way as you connect directly to the database. The main difference is that you specify the proxy endpoint instead of the instance or cluster endpoint. For an Aurora DB cluster, by default all proxy connections have read/write capability and use the writer instance. If you normally use the reader endpoint for read-only connections, you can create an additional read-only endpoint for the proxy. You can use that endpoint the same way. For more information, see [Overview of proxy endpoints \(p. 953\)](#).

Topics

- [Connecting to a proxy using native authentication \(p. 939\)](#)
- [Connecting to a proxy using IAM authentication \(p. 940\)](#)
- [Considerations for connecting to a proxy with Microsoft SQL Server \(p. 940\)](#)
- [Considerations for connecting to a proxy with PostgreSQL \(p. 941\)](#)

Connecting to a proxy using native authentication

Use the following basic steps to connect to a proxy using native authentication:

1. Find the proxy endpoint. In the AWS Management Console, you can find the endpoint on the details page for the corresponding proxy. With the AWS CLI, you can use the [describe-db-proxies](#) command. The following example shows how.

```
# Add --output text to get output as a simple tab-separated list.
$ aws rds describe-db-proxies --query '*[*].{DBProxyName:DBProxyName,Endpoint:Endpoint}'
[
    [
        {
            "Endpoint": "the-proxy.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy"
        },
        {
            "Endpoint": "the-proxy-other-secret.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-other-secret"
        },
        {
            "Endpoint": "the-proxy-rds-secret.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-rds-secret"
        },
        {
            "Endpoint": "the-proxy-t3.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-t3"
        }
    ]
]
```

2. Specify that endpoint as the host parameter in the connection string for your client application. For example, specify the proxy endpoint as the value for the mysql -h option or psql -h option.
3. Supply the same database user name and password as you usually do.

Connecting to a proxy using IAM authentication

When you use IAM authentication with RDS Proxy, set up your database users to authenticate with regular user names and passwords. The IAM authentication applies to RDS Proxy retrieving the user name and password credentials from Secrets Manager. The connection from RDS Proxy to the underlying database doesn't go through IAM.

To connect to RDS Proxy using IAM authentication, use the same general connection procedure as for IAM authentication with an RDS DB instance or Aurora cluster. For general information about using IAM with RDS and Aurora, see [Security in Amazon RDS \(p. 1997\)](#).

The major differences in IAM usage for RDS Proxy include the following:

- You don't configure each individual database user with an authorization plugin. The database users still have regular user names and passwords within the database. You set up Secrets Manager secrets containing these user names and passwords, and authorize RDS Proxy to retrieve the credentials from Secrets Manager.

The IAM authentication applies to the connection between your client program and the proxy. The proxy then authenticates to the database using the user name and password credentials retrieved from Secrets Manager.

- Instead of the instance, cluster, or reader endpoint, you specify the proxy endpoint. For details about the proxy endpoint, see [Connecting to your DB instance using IAM authentication \(p. 2055\)](#).
- In the direct database IAM authentication case, you selectively choose database users and configure them to be identified with a special authentication plugin. You can then connect to those users using IAM authentication.

In the proxy use case, you provide the proxy with Secrets that contain some user's user name and password (native authentication). You then connect to the proxy using IAM authentication. Here, you do this by generating an authentication token with the proxy endpoint, not the database endpoint. You also use a user name that matches one of the user names for the secrets that you provided.

- Make sure that you use Transport Layer Security (TLS)/Secure Sockets Layer (SSL) when connecting to a proxy using IAM authentication.

You can grant a specific user access to the proxy by modifying the IAM policy. An example follows.

```
"Resource": "arn:aws:rds-db:us-east-2:1234567890:dbuser:px-ABCDEFGHIJKLM01234/db_user"
```

Considerations for connecting to a proxy with Microsoft SQL Server

For connecting to a proxy using IAM authentication, you don't use the password field. Instead, you provide the appropriate token property for each type of database driver in the token field. For example, use the accessToken property for JDBC, or the sql_copt_ss_access_token property for ODBC. Or use the AccessToken property for the .NET SqlClient driver. You can't use IAM authentication with clients that don't support token properties.

Under some conditions, a proxy can't share a database connection and instead pins the connection from your client application to the proxy to a dedicated database connection. For more information about these conditions, see [Avoiding pinning \(p. 948\)](#).

Considerations for connecting to a proxy with PostgreSQL

For PostgreSQL, when a client starts a connection to a PostgreSQL database, it sends a startup message. This message includes pairs of parameter name and value strings. For details, see the [StartupMessage](#) in [PostgreSQL message formats](#) in the PostgreSQL documentation.

When connecting through an RDS proxy, the startup message can include the following currently recognized parameters:

- `user`
- `database`
- `replication`

The startup message can also include the following additional runtime parameters:

- `application_name`
- `client_encoding`
- `DateStyle`
- `TimeZone`
- `extra_float_digits`

For more information about PostgreSQL messaging, see the [Frontend/Backend protocol](#) in the PostgreSQL documentation.

For PostgreSQL, if you use JDBC we recommend the following to avoid pinning:

- Set the JDBC connection parameter `assumeMinServerVersion` to at least `9.0` to avoid pinning. Doing this prevents the JDBC driver from performing an extra round trip during connection startup when it runs `SET extra_float_digits = 3`.
- Set the JDBC connection parameter `ApplicationName` to `any/your-application-name` to avoid pinning. Doing this prevents the JDBC driver from performing an extra round trip during connection startup when it runs `SET application_name = "PostgreSQL JDBC Driver"`. Note the JDBC parameter is `ApplicationName` but the PostgreSQL `StartupMessage` parameter is `application_name`.
- Set the JDBC connection parameter `preferQueryMode` to `extendedForPrepared` to avoid pinning. The `extendedForPrepared` ensures that the extended mode is used only for prepared statements.

The default for the `preferQueryMode` parameter is `extended`, which uses the extended mode for all queries. The extended mode uses a series of `Prepare`, `Bind`, `Execute`, and `Sync` requests and corresponding responses. This type of series causes connection pinning in an RDS proxy.

For more information, see [Avoiding pinning \(p. 948\)](#). For more information about connecting using JDBC, see [Connecting to the database](#) in the PostgreSQL documentation.

Managing an RDS Proxy

Following, you can find an explanation of how to manage RDS Proxy operation and configuration. These procedures help your application make the most efficient use of database connections and achieve maximum connection reuse. The more that you can take advantage of connection reuse, the more CPU and memory overhead that you can save. This in turn reduces latency for your application and enables the database to devote more of its resources to processing application requests.

Topics

- [Modifying an RDS Proxy \(p. 942\)](#)
- [Adding a new database user \(p. 946\)](#)
- [Changing the password for a database user \(p. 946\)](#)
- [Configuring connection settings \(p. 946\)](#)
- [Avoiding pinning \(p. 948\)](#)
- [Deleting an RDS Proxy \(p. 952\)](#)

Modifying an RDS Proxy

You can change certain settings associated with a proxy after you create the proxy. You do so by modifying the proxy itself, its associated target group, or both. Each proxy has an associated target group.

AWS Management Console

To modify the settings for a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. In the list of proxies, choose the proxy whose settings you want to modify or go to its details page.
4. For **Actions**, choose **Modify**.
5. Enter or choose the properties to modify. You can modify the following:
 - **Proxy identifier** – Rename the proxy by entering a new identifier.
 - **Require Transport Layer Security** – Turn the requirement for Transport layer Security (TLS) on or off.
 - **Idle client connection timeout** – Enter a time period for the idle client connection timeout.
 - **Secrets Manager secrets** – Add or remove Secrets Manager secrets. These secrets correspond to database user names and passwords.
 - **IAM role** – Change the IAM role used to retrieve the secrets from Secrets Manager.
 - **IAM Authentication** – Require or disallow IAM authentication for connections to the proxy.
 - **VPC security group** – Add or remove VPC security groups for the proxy to use.
 - **Enable enhanced logging** – Enable or disable enhanced logging.
6. Choose **Modify**.

If you didn't find the settings listed that you want to change, use the following procedure to update the target group for the proxy. The *target group* associated with a proxy controls the settings related to the physical database connections. Each proxy has one associated target group named **default**, which is created automatically along with the proxy.

You can only modify the target group from the proxy details page, not from the list on the **Proxies** page.

To modify the settings for a proxy target group

1. On the **Proxies** page, go to the details page for a proxy.
2. For **Target groups**, choose the **default** link. Currently, all proxies have a single target group named **default**.
3. On the details page for the **default** target group, choose **Modify**.
4. Choose new settings for the properties that you can modify:

- **Database** – Choose a different RDS DB instance or Aurora cluster.
- **Connection pool maximum connections** – Adjust what percentage of the maximum available connections the proxy can use.
- **Session pinning filters** – (Optional) Choose a session pinning filter. Doing this can help reduce performance issues due to insufficient transaction-level reuse for connections. Using this setting requires understanding of application behavior and the circumstances under which RDS Proxy pins a session to a database connection. Currently, the setting isn't supported for PostgreSQL and the only choice is EXCLUDE_VARIABLE_SETS.
- **Connection borrow timeout** – Adjust the connection borrow timeout interval. This setting applies when the maximum number of connections is already being used for the proxy. The setting determines how long the proxy waits for a connection to become available before returning a timeout error.
- **Initialization query** – (Optional) Add an initialization query, or modify the current one. You can specify one or more SQL statements for the proxy to run when opening each new database connection. The setting is typically used with SET statements to make sure that each connection has identical settings such as time zone and character set. For multiple statements, use semicolons as the separator. You can also include multiple variables in a single SET statement, such as SET x=1, y=2. Initialization query is not currently supported for PostgreSQL.

You can't change certain properties, such as the target group identifier and the database engine.

5. Choose **Modify target group**.

AWS CLI

To modify a proxy using the AWS CLI, use the commands [modify-db-proxy](#), [modify-db-proxy-target-group](#), [deregister-db-proxy-targets](#), and [register-db-proxy-targets](#).

With the `modify-db-proxy` command, you can change properties such as the following:

- The set of Secrets Manager secrets used by the proxy.
- Whether TLS is required.
- The idle client timeout.
- Whether to log additional information from SQL statements for debugging.
- The IAM role used to retrieve Secrets Manager secrets.
- The security groups used by the proxy.

The following example shows how to rename an existing proxy.

```
aws rds modify-db-proxy --db-proxy-name the-proxy --new-db-proxy-name the_new_name
```

To modify connection-related settings or rename the target group, use the `modify-db-proxy-target-group` command. Currently, all proxies have a single target group named default. When working with this target group, you specify the name of the proxy and default for the name of the target group.

The following example shows how to first check the `MaxIdleConnectionsPercent` setting for a proxy and then change it, using the target group.

```
aws rds describe-db-proxy-target-groups --db-proxy-name the-proxy
{
    "TargetGroups": [
```

```
{
    "Status": "available",
    "UpdatedDate": "2019-11-30T16:49:30.342Z",
    "ConnectionPoolConfig": {
        "MaxIdleConnectionsPercent": 50,
        "ConnectionBorrowTimeout": 120,
        "MaxConnectionsPercent": 100,
        "SessionPinningFilters": []
    },
    "TargetGroupName": "default",
    "CreatedDate": "2019-11-30T16:49:27.940Z",
    "DBProxyName": "the-proxy",
    "IsDefault": true
}
]

}

aws rds modify-db-proxy-target-group --db-proxy-name the-proxy --target-group-name default
--connection-pool-config '
{ "MaxIdleConnectionsPercent": 75 }'

{
    "DBProxyTargetGroup": {
        "Status": "available",
        "UpdatedDate": "2019-12-02T04:09:50.420Z",
        "ConnectionPoolConfig": {
            "MaxIdleConnectionsPercent": 75,
            "ConnectionBorrowTimeout": 120,
            "MaxConnectionsPercent": 100,
            "SessionPinningFilters": []
        },
        "TargetGroupName": "default",
        "CreatedDate": "2019-11-30T16:49:27.940Z",
        "DBProxyName": "the-proxy",
        "IsDefault": true
    }
}
```

With the `deregister-db-proxy-targets` and `register-db-proxy-targets` commands, you change which RDS DB instance or Aurora DB cluster the proxy is associated with through its target group. Currently, each proxy can connect to one RDS DB instance or Aurora DB cluster. The target group tracks the connection details for all the RDS DB instances in a Multi-AZ configuration. Or the target group tracks the connection details for all the DB instances in an Aurora cluster.

The following example starts with a proxy that is associated with an Aurora MySQL cluster named `cluster-56-2020-02-25-1399`. The example shows how to change the proxy so that it can connect to a different cluster named `provisioned-cluster`.

When you work with an RDS DB instance, you specify the `--db-instance-identifier` option. When you work with an Aurora DB cluster, you specify the `--db-cluster-identifier` option instead.

The following example modifies an Aurora MySQL proxy. An Aurora PostgreSQL proxy has port 5432.

```
aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": [
        {
            "Endpoint": "instance-9814.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-9814"
        },
        {

```

```

        "Endpoint": "instance-8898.demo.us-east-1.rds.amazonaws.com",
        "Type": "RDS_INSTANCE",
        "Port": 3306,
        "RdsResourceId": "instance-8898"
    },
    {
        "Endpoint": "instance-1018.demo.us-east-1.rds.amazonaws.com",
        "Type": "RDS_INSTANCE",
        "Port": 3306,
        "RdsResourceId": "instance-1018"
    },
    {
        "Type": "TRACKED_CLUSTER",
        "Port": 0,
        "RdsResourceId": "cluster-56-2020-02-25-1399"
    },
    {
        "Endpoint": "instance-4330.demo.us-east-1.rds.amazonaws.com",
        "Type": "RDS_INSTANCE",
        "Port": 3306,
        "RdsResourceId": "instance-4330"
    }
]
}

aws rds deregister-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
cluster-56-2020-02-25-1399

aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": []
}

aws rds register-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
provisioned-cluster

{
    "DBProxyTargets": [
        {
            "Type": "TRACKED_CLUSTER",
            "Port": 0,
            "RdsResourceId": "provisioned-cluster"
        },
        {
            "Endpoint": "gkldje.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "gkldje"
        },
        {
            "Endpoint": "provisioned-1.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "provisioned-1"
        }
    ]
}

```

RDS API

To modify a proxy using the RDS API, you use the operations [ModifyDBProxy](#), [ModifyDBProxyTargetGroup](#), [DeregisterDBProxyTargets](#), and [RegisterDBProxyTargets](#) operations.

With [ModifyDBProxy](#), you can change properties such as the following:

- The set of Secrets Manager secrets used by the proxy.
- Whether TLS is required.
- The idle client timeout.
- Whether to log additional information from SQL statements for debugging.
- The IAM role used to retrieve Secrets Manager secrets.
- The security groups used by the proxy.

With `ModifyDBProxyTargetGroup`, you can modify connection-related settings or rename the target group. Currently, all proxies have a single target group named `default`. When working with this target group, you specify the name of the proxy and `default` for the name of the target group.

With `DeregisterDBProxyTargets` and `RegisterDBProxyTargets`, you change which RDS DB instance or Aurora DB cluster the proxy is associated with through its target group. Currently, each proxy can connect to one RDS DB instance or Aurora DB cluster. The target group tracks the connection details for all the RDS DB instances in a Multi-AZ configuration, or all the DB instances in an Aurora cluster.

Adding a new database user

In some cases, you might add a new database user to an RDS DB instance or Aurora cluster that's associated with a proxy. If so, add or repurpose a Secrets Manager secret to store the credentials for that user. To do this, choose one of the following options:

- Create a new Secrets Manager secret, using the procedure described in [Setting up database credentials in AWS Secrets Manager \(p. 931\)](#).
- Update the IAM role to give RDS Proxy access to the new Secrets Manager secret. To do so, update the resources section of the IAM role policy.
- If the new user takes the place of an existing one, update the credentials stored in the proxy's Secrets Manager secret for the existing user.

Changing the password for a database user

In some cases, you might change the password for a database user in an RDS DB instance or Aurora cluster that's associated with a proxy. If so, update the corresponding Secrets Manager secret with the new password.

Configuring connection settings

To adjust RDS Proxy's connection pooling, you can modify the following settings:

- [IdleClientTimeout \(p. 946\)](#)
- [MaxConnectionsPercent \(p. 947\)](#)
- [MaxIdleConnectionsPercent \(p. 947\)](#)
- [ConnectionBorrowTimeout \(p. 947\)](#)

IdleClientTimeout

You can specify how long a client connection can be idle before the proxy can close it. The default is 1,800 seconds (30 minutes).

A client connection is considered *idle* when the application doesn't submit a new request within the specified time after the previous request completed. The underlying database connection stays open and is returned to the connection pool. Thus, it's available to be reused for new client connections. If

you want the proxy to proactively remove stale connections, consider lowering the idle client connection timeout. If your workload establishes frequent connections with the proxy, consider raising the idle client connection timeout to save the cost of establishing connections.

This setting is represented by the **Idle client connection timeout** field in the RDS console and the `IdleClientTimeout` setting in the AWS CLI and the API. To learn how to change the value of the **Idle client connection timeout** field in the RDS console, see [AWS Management Console \(p. 942\)](#). To learn how to change the value of the `IdleClientTimeout` setting, see the CLI command [modify-db-proxy](#) or the API operation [ModifyDBProxy](#).

MaxConnectionsPercent

You can limit the number of connections that an RDS Proxy can establish with the database. You specify the limit as a percentage of the maximum connections available for your database. The proxy doesn't create all of these connections in advance. This setting reserves the right for the proxy to establish these connections as the workload needs them.

For example, suppose that you configured RDS Proxy to use 75 percent of the maximum connections for your database. In this case, your database supports a maximum of 1,000 concurrent connections. Here, RDS Proxy can open up to 750 database connections.

This setting is represented by the **Connection pool maximum connections** field in the RDS console and the `MaxConnectionsPercent` setting in the AWS CLI and the API. To learn how to change the value of the **Connection pool maximum connections** field in the RDS console, see [AWS Management Console \(p. 942\)](#). To learn how to change the value of the `MaxConnectionsPercent` setting, see the CLI command [modify-db-proxy-target-group](#) or the API operation [ModifyDBProxyTargetGroup](#).

For information on database connection limits, see [Maximum number of database connections](#).

MaxIdleConnectionsPercent

You can control the number of idle database connections that RDS Proxy can keep in the connection pool. RDS Proxy considers a database connection in its pool to be *idle* when there's been no activity on the connection for five minutes.

You specify the limit as a percentage of the maximum connections available for your database. The default value is 50 percent of `MaxConnectionsPercent`, and the upper limit is the value of `MaxConnectionsPercent`. With a high value, the proxy leaves a high percentage of idle database connections open. With a low value, the proxy closes a high percentage of idle database connections. If your workloads are unpredictable, consider setting a high value for `MaxIdleConnectionsPercent`. Doing so means that RDS Proxy can accommodate surges in activity without opening a lot of new database connections.

This setting is represented by the `MaxIdleConnectionsPercent` setting of `DBProxyTargetGroup` in the AWS CLI and the API. To learn how to change the value of the `MaxIdleConnectionsPercent` setting, see the CLI command [modify-db-proxy-target-group](#) or the API operation [ModifyDBProxyTargetGroup](#).

Note

RDS Proxy closes database connections some time after 24 hours when they are no longer in use. The proxy performs this action regardless of the value of the maximum idle connections setting.

For information on database connection limits, see [Maximum number of database connections](#).

ConnectionBorrowTimeout

You can choose how long RDS Proxy waits for a database connection in the connection pool to become available for use before returning a timeout error. The default is 120 seconds. This setting applies when

the number of connections is at the maximum, and so no connections are available in the connection pool. It also applies if no appropriate database instance is available to handle the request because, for example, a failover operation is in process. Using this setting, you can set the best wait period for your application without having to change the query timeout in your application code.

This setting is represented by the **Connection borrow timeout** field in the RDS console or the `ConnectionBorrowTimeout` setting of `DBProxyTargetGroup` in the AWS CLI or API. To learn how to change the value of the **Connection borrow timeout** field in the RDS console, see [AWS Management Console \(p. 942\)](#). To learn how to change the value of the `ConnectionBorrowTimeout` setting, see the CLI command `modify-db-proxy-target-group` or the API operation `ModifyDBProxyTargetGroup`.

Avoiding pinning

Multiplexing is more efficient when database requests don't rely on state information from previous requests. In that case, RDS Proxy can reuse a connection at the conclusion of each transaction. Examples of such state information include most variables and configuration parameters that you can change through `SET` or `SELECT` statements. SQL transactions on a client connection can multiplex between underlying database connections by default.

Your connections to the proxy can enter a state known as *pinning*. When a connection is pinned, each later transaction uses the same underlying database connection until the session ends. Other client connections also can't reuse that database connection until the session ends. The session ends when the client connection is dropped.

RDS Proxy automatically pins a client connection to a specific DB connection when it detects a session state change that isn't appropriate for other sessions. Pinning reduces the effectiveness of connection reuse. If all or almost all of your connections experience pinning, consider modifying your application code or workload to reduce the conditions that cause the pinning.

For example, suppose that your application changes a session variable or configuration parameter. In this case, later statements can rely on the new variable or parameter to be in effect. Thus, when RDS Proxy processes requests to change session variables or configuration settings, it pins that session to the DB connection. That way, the session state remains in effect for all later transactions in the same session.

For some database engines, this rule doesn't apply to all parameters that you can set. RDS Proxy tracks certain statements and variables. Thus RDS Proxy doesn't pin the session when you modify them. In this case, RDS Proxy only reuses the connection for other sessions that have the same values for those settings. For details about what RDS Proxy tracks for a database engine, see the following:

- [What RDS Proxy tracks for RDS for SQL Server databases \(p. 948\)](#)
- [What RDS Proxy tracks for RDS for MariaDB and RDS for MySQL databases \(p. 949\)](#)

What RDS Proxy tracks for RDS for SQL Server databases

Following are the SQL Server statements that RDS Proxy tracks:

- `USE`
- `SET ANSI_NULLS`
- `SET ANSI_PADDING`
- `SET ANSI_WARNINGS`
- `SET ARITHABORT`
- `SET CONCAT_NULL_YIELDS_NULL`
- `SET CURSOR_CLOSE_ON_COMMIT`
- `SET DATEFIRST`

- SET DATEFORMAT
- SET LANGUAGE
- SET LOCK_TIMEOUT
- SET NUMERIC_ROUNDABORT
- SET QUOTED_IDENTIFIER
- SET TEXTSIZE
- SET TRANSACTION ISOLATION LEVEL

What RDS Proxy tracks for RDS for MariaDB and RDS for MySQL databases

Following are the MySQL and MariaDB statements that RDS Proxy tracks:

- DROP DATABASE
- DROP SCHEMA
- USE

Following are the MySQL and MariaDB variables that RDS Proxy tracks:

- AUTOCOMMIT
- AUTO_INCREMENT_INCREMENT
- CHARACTER_SET (or CHAR_SET)
- CHARACTER_SET_CLIENT
- CHARACTER_SET_DATABASE
- CHARACTER_SET_FILESYSTEM
- CHARACTER_SET_CONNECTION
- CHARACTER_SET_RESULTS
- CHARACTER_SET_SERVER
- COLLATION_CONNECTION
- COLLATION_DATABASE
- COLLATION_SERVER
- INTERACTIVE_TIMEOUT
- NAMES
- NET_WRITE_TIMEOUT
- QUERY_CACHE_TYPE
- SESSION_TRACK_SCHEMA
- SQL_MODE
- TIME_ZONE
- TRANSACTION_ISOLATION (or TX_ISOLATION)
- TRANSACTION_READ_ONLY (or TX_READ_ONLY)
- WAIT_TIMEOUT

Minimizing pinning

Performance tuning for RDS Proxy involves trying to maximize transaction-level connection reuse (multiplexing) by minimizing pinning.

In some cases, RDS Proxy can't be sure that it's safe to reuse a database connection outside of the current session. In these cases, it keeps the session on the same connection until the session ends. This fallback behavior is called *pinning*.

You can minimize pinning by doing the following:

- Avoid unnecessary database requests that might cause pinning.
- Set variables and configuration settings consistently across all connections. That way, later sessions are more likely to reuse connections that have those particular settings.

However, for PostgreSQL setting a variable leads to session pinning.

- For a MySQL engine family database, apply a session pinning filter to the proxy. You can exempt certain kinds of operations from pinning the session if you know that doing so doesn't affect the correct operation of your application.
- See how frequently pinning occurs by monitoring the Amazon CloudWatch metric `DatabaseConnectionsCurrentlySessionPinned`. For information about this and other CloudWatch metrics, see [Monitoring RDS Proxy metrics with Amazon CloudWatch \(p. 959\)](#).
- If you use SET statements to perform identical initialization for each client connection, you can do so while preserving transaction-level multiplexing. In this case, you move the statements that set up the initial session state into the initialization query used by a proxy. This property is a string containing one or more SQL statements, separated by semicolons.

For example, you can define an initialization query for a proxy that sets certain configuration parameters. Then, RDS Proxy applies those settings whenever it sets up a new connection for that proxy. You can remove the corresponding SET statements from your application code, so that they don't interfere with transaction-level multiplexing.

For metrics about how often pinning occurs for a proxy, see [Monitoring RDS Proxy metrics with Amazon CloudWatch \(p. 959\)](#).

Conditions that cause pinning for all engine families

The proxy pins the session to the current connection in the following situations where multiplexing might cause unexpected behavior:

- Any statement with a text size greater than 16 KB causes the proxy to pin the session.
- Prepared statements cause the proxy to pin the session. This rule applies whether the prepared statement uses SQL text or the binary protocol.

Conditions that cause pinning for RDS for Microsoft SQL Server

For RDS for SQL Server, the following interactions also cause pinning:

- Using multiple active result sets (MARS). For information about MARS, see the [SQL Server documentation](#).
- Using distributed transaction coordinator (DTC) communication.
- Creating temporary tables, transactions, cursors, or prepared statements.
- Using the following SET statements:
 - SET ANSI_DEFAULTS
 - SET ANSI_NULL_DFLT
 - SET ARITHIGNORE
 - SET DEADLOCK_PRIORITY
 - SET FIPS_FLAGGER

- SET FMTONLY
- SET FORCEPLAN
- SET IDENTITY_INSERT
- SET NOCOUNT
- SET NOEXEC
- SET OFFSETS
- SET PARSEONLY
- SET QUERY_GOVERNOR_COST_LIMIT
- SET REMOTE_PROC_TRANSACTIONS
- SET ROWCOUNT
- SET SHOWPLAN_ALL, SHOWPLAN_TEXT, and SHOWPLAN_XML
- SET STATISTICS
- SET XACT_ABORT

Conditions that cause pinning for RDS for MariaDB and RDS for MySQL

For MySQL and MariaDB, the following interactions also cause pinning:

- Explicit table lock statements LOCK TABLE, LOCK TABLES, or FLUSH TABLES WITH READ LOCK cause the proxy to pin the session.
- Creating named locks by using GET_LOCK causes the proxy to pin the session.
- Setting a user variable or a system variable (with some exceptions) causes the proxy to pin the session. If this situation reduces your connection reuse too much, you can choose for SET operations not to cause pinning. For information about how to do so by setting the session pinning filters property, see [Creating an RDS Proxy \(p. 934\)](#) and [Modifying an RDS Proxy \(p. 942\)](#).
- Creating a temporary table causes the proxy to pin the session. That way, the contents of the temporary table are preserved throughout the session regardless of transaction boundaries.
- Calling the functions ROW_COUNT, FOUND_ROWS, and LAST_INSERT_ID sometimes causes pinning.

Calling stored procedures and stored functions doesn't cause pinning. RDS Proxy doesn't detect any session state changes resulting from such calls. Therefore, make sure that your application doesn't change session state inside stored routines and rely on that session state to persist across transactions. For example, if a stored procedure creates a temporary table that is intended to persist across transactions, that application currently isn't compatible with RDS Proxy.

If you have expert knowledge about your application behavior, you can skip the pinning behavior for certain application statements. To do so, choose the **Session pinning filters** option when creating the proxy. Currently, you can opt out of session pinning for setting session variables and configuration settings.

Conditions that cause pinning for RDS for PostgreSQL

For PostgreSQL, the following interactions also cause pinning:

- Using SET commands
- Using the PostgreSQL extended query protocol such as by using JDBC default settings
- Creating temporary sequences, tables, or views
- Declaring cursors
- Discarding the session state

- Listening on a notification channel
- Loading a library module such as auto_explain
- Manipulating sequences using functions such as nextval and setval
- Interacting with locks using functions such as pg_advisory_lock and pg_try_advisory_lock
- Using prepared statements, setting parameters, or resetting a parameter to its default

Deleting an RDS Proxy

You can delete a proxy if you no longer need it. You might delete a proxy because the application that was using it is no longer relevant. Or you might delete a proxy if you take the DB instance or cluster associated with it out of service.

AWS Management Console

To delete a proxy

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. Choose the proxy to delete from the list.
4. Choose **Delete Proxy**.

AWS CLI

To delete a DB proxy, use the AWS CLI command `delete-db-proxy`. To remove related associations, also use the `deregister-db-proxy-targets` command.

```
aws rds delete-db-proxy --name proxy_name
```

```
aws rds deregister-db-proxy-targets
  --db-proxy-name proxy_name
  [--target-group-name target_group_name]
  [--target-ids comma_separated_list]      # or
  [--db-instance-identifiers instance_id]      # or
  [--db-cluster-identifiers cluster_id]
```

RDS API

To delete a DB proxy, call the Amazon RDS API function `DeleteDBProxy`. To delete related items and associations, you also call the functions `DeleteDBProxyTargetGroup` and `DeregisterDBProxyTargets`.

Working with Amazon RDS Proxy endpoints

Following, you can learn about endpoints for RDS Proxy and how to use them. By using endpoints, you can take advantage of the following capabilities:

- You can use multiple endpoints with a proxy to monitor and troubleshoot connections from different applications independently.
- You can use reader endpoints with Aurora DB clusters to improve read scalability and high availability for your query-intensive applications.
- You can use a cross-VPC endpoint to allow access to databases in one VPC from resources such as Amazon EC2 instances in a different VPC.

Topics

- [Overview of proxy endpoints \(p. 953\)](#)
- [Reader endpoints \(p. 953\)](#)
- [Accessing Aurora and RDS databases across VPCs \(p. 954\)](#)
- [Creating a proxy endpoint \(p. 954\)](#)
- [Viewing proxy endpoints \(p. 956\)](#)
- [Modifying a proxy endpoint \(p. 957\)](#)
- [Deleting a proxy endpoint \(p. 958\)](#)
- [Limitations for proxy endpoints \(p. 959\)](#)

Overview of proxy endpoints

Working with RDS Proxy endpoints involves the same kinds of procedures as with Aurora DB cluster and reader endpoints and RDS instance endpoints. If you aren't familiar with RDS endpoints, find more information in [Connecting to a DB instance running the MySQL database engine](#) and [Connecting to a DB instance running the PostgreSQL database engine](#).

By default, the endpoint that you connect to when you use RDS Proxy with an Aurora cluster has read/write capability. As a result, this endpoint sends all requests to the writer instance of the cluster. All of those connections count against the `max_connections` value for the writer instance. If your proxy is associated with an Aurora DB cluster, you can create additional read/write or read-only endpoints for that proxy.

You can use a read-only endpoint with your proxy for read-only queries. You do this the same way that you use the reader endpoint for an Aurora provisioned cluster. Doing so helps you to take advantage of the read scalability of an Aurora cluster with one or more reader DB instances. You can run more simultaneous queries and make more simultaneous connections by using a read-only endpoint and adding more reader DB instances to your Aurora cluster as needed.

For a proxy endpoint that you create, you can also associate the endpoint with a different virtual private cloud (VPC) than the proxy itself uses. By doing so, you can connect to the proxy from a different VPC, for example a VPC used by a different application within your organization.

For information about limits associated with proxy endpoints, see [Limitations for proxy endpoints \(p. 959\)](#).

In the RDS Proxy logs, each entry is prefixed with the name of the associated proxy endpoint. This name can be the name you specified for a user-defined endpoint. Or it can be the special name `default` for read/write requests using the default endpoint of a proxy.

Each proxy endpoint has its own set of CloudWatch metrics. You can monitor the metrics for all endpoints of a proxy. You can also monitor metrics for a specific endpoint, or for all the read/write or read-only endpoints of a proxy. For more information, see [Monitoring RDS Proxy metrics with Amazon CloudWatch \(p. 959\)](#).

A proxy endpoint uses the same authentication mechanism as its associated proxy. RDS Proxy automatically sets up permissions and authorizations for the user-defined endpoint, consistent with the properties of the associated proxy.

Reader endpoints

With RDS Proxy, you can create and use reader endpoints. However, these endpoints only work for proxies associated with Aurora DB clusters. You might see references to reader endpoints in the AWS

Management Console. If you use the RDS CLI or API, you might see the `TargetRole` attribute with a value of `READ_ONLY`. You can take advantage of these features by changing the target of a proxy from an RDS DB instance to an Aurora DB cluster. To learn about reader endpoints, see [Managing connections with Amazon RDS Proxy](#) in the *Aurora User Guide*.

Accessing Aurora and RDS databases across VPCs

By default, the components of your RDS and Aurora technology stack are all in the same Amazon VPC. For example, suppose that an application running on an Amazon EC2 instance connects to an Amazon RDS DB instance or an Aurora DB cluster. In this case, the application server and database must both be within the same VPC.

With RDS Proxy, you can set up access to an Aurora cluster or RDS instance in one VPC from resources such as EC2 instances in another VPC. For example, your organization might have multiple applications that access the same database resources. Each application might be in its own VPC.

To enable cross-VPC access, you create a new endpoint for the proxy. If you aren't familiar with creating proxy endpoints, see [Working with Amazon RDS Proxy endpoints \(p. 952\)](#) for details. The proxy itself resides in the same VPC as the Aurora DB cluster or RDS instance. However, the cross-VPC endpoint resides in the other VPC, along with the other resources such as the EC2 instances. The cross-VPC endpoint is associated with subnets and security groups from the same VPC as the EC2 and other resources. These associations let you connect to the endpoint from the applications that otherwise can't access the database due to the VPC restrictions.

The following steps explain how to create and access a cross-VPC endpoint through RDS Proxy:

1. Create two VPCs, or choose two VPCs that you already use for Aurora and RDS work. Each VPC should have its own associated network resources such as an Internet gateway, route tables, subnets, and security groups. If you only have one VPC, you can consult [Getting started with Amazon RDS \(p. 153\)](#) for the steps to set up another VPC to use RDS successfully. You can also examine your existing VPC in the Amazon EC2 console to see what kinds of resources to connect together.
2. Create a DB proxy associated with the Aurora DB cluster or RDS instance that you want to connect to. Follow the procedure in [Creating an RDS Proxy \(p. 934\)](#).
3. On the **Details** page for your proxy in the RDS console, under the **Proxy endpoints** section, choose **Create endpoint**. Follow the procedure in [Creating a proxy endpoint \(p. 954\)](#).
4. Choose whether to make the cross-VPC endpoint read/write or read-only.
5. Instead of accepting the default of the same VPC as the Aurora DB cluster or RDS instance, choose a different VPC. This VPC must be in the same AWS Region as the VPC where the proxy resides.
6. Now instead of accepting the defaults for subnets and security groups from the same VPC as the Aurora DB cluster or RDS instance, make new selections. Make these based on the subnets and security groups from the VPC that you chose.
7. You don't need to change any of the settings for the Secrets Manager secrets. The same credentials work for all endpoints for your proxy, regardless of which VPC each endpoint is in.
8. Wait for the new endpoint to reach the **Available** state.
9. Make a note of the full endpoint name. This is the value ending in `Region_name.rds.amazonaws.com` that you supply as part of the connection string for your database application.
10. Access the new endpoint from a resource in the same VPC as the endpoint. A simple way to test this process is to create a new EC2 instance in this VPC. Then you can log into the EC2 instance and run the `mysql` or `psql` commands to connect by using the endpoint value in your connection string.

Creating a proxy endpoint

Console

To create a proxy endpoint

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. Click the name of the proxy that you want to create a new endpoint for.

The details page for that proxy appears.

4. In the **Proxy endpoints** section, choose **Create proxy endpoint**.

The **Create proxy endpoint** window appears.

5. For **Proxy endpoint name**, enter a descriptive name of your choice.
6. For **Target role**, choose whether to make the endpoint read/write or read-only.

Connections that use a read/write endpoint can perform any kind of operation: data definition language (DDL) statements, data manipulation language (DML) statements, and queries. These endpoints always connect to the primary instance of the Aurora cluster. You can use read/write endpoints for general database operations when you only use a single endpoint in your application. You can also use read/write endpoints for administrative operations, online transaction processing (OLTP) applications, and extract-transform-load (ETL) jobs.

Connections that use a read-only endpoint can only perform queries. When there are multiple reader instances in the Aurora cluster, RDS Proxy can use a different reader instance for each connection to the endpoint. That way, a query-intensive application can take advantage of Aurora's clustering capability. You can add more query capacity to the cluster by adding more reader DB instances. These read-only connections don't impose any overhead on the primary instance of the cluster. That way, your reporting and analysis queries don't slow down the write operations of your OLTP applications.

7. For **Virtual Private Cloud (VPC)**, choose the default to access the endpoint from the same EC2 instances or other resources where you normally access the proxy or its associated database. To set up cross-VPC access for this proxy, choose a VPC other than the default. For more information about cross-VPC access, see [Accessing Aurora and RDS databases across VPCs \(p. 954\)](#).
8. For **Subnets**, RDS Proxy fills in the same subnets as the associated proxy by default. To restrict access to the endpoint so only a portion of the VPC's address range can connect to it, remove one or more subnets.
9. For **VPC security group**, you can choose an existing security group or create a new one. RDS Proxy fills in the same security group or groups as the associated proxy by default. If the inbound and outbound rules for the proxy are appropriate for this endpoint, you can leave the default choice.

If you choose to create a new security group, specify a name for the security group on this page. Then edit the security group settings from the EC2 console afterward.

10. Choose **Create proxy endpoint**.

AWS CLI

To create a proxy endpoint, use the AWS CLI [create-db-proxy-endpoint](#) command.

Include the following required parameters:

- `--db-proxy-name value`
- `--db-proxy-endpoint-name value`
- `--vpc-subnet-ids list_of_ids`. Separate the subnet IDs with spaces. You don't specify the ID of the VPC itself.

You can also include the following optional parameters:

- `--target-role` { READ_WRITE | READ_ONLY }. This parameter defaults to READ_WRITE. The READ_ONLY value only has an effect on Aurora provisioned clusters that contain one or more reader DB instances. When the proxy is associated with an RDS instance or with an Aurora cluster that only contains a writer DB instance, you can't specify READ_ONLY.
- `--vpc-security-group-ids` *value*. Separate the security group IDs with spaces. If you omit this parameter, RDS Proxy uses the default security group for the VPC. RDS Proxy determines the VPC based on the subnet IDs that you specify for the `--vpc-subnet-ids` parameter.

Example

The following example creates a proxy endpoint named `my-endpoint`.

For Linux, macOS, or Unix:

```
aws rds create-db-proxy-endpoint \
--db-proxy-name my-proxy \
--db-proxy-endpoint-name my-endpoint \
--vpc-subnet-ids subnet_id subnet_id subnet_id ... \
--target-role READ_ONLY \
--vpc-security-group-ids security_group_id ]
```

For Windows:

```
aws rds create-db-proxy-endpoint ^
--db-proxy-name my-proxy ^
--db-proxy-endpoint-name my-endpoint ^
--vpc-subnet-ids subnet_id_1 subnet_id_2 subnet_id_3 ... ^
--target-role READ_ONLY ^
--vpc-security-group-ids security_group_id
```

RDS API

To create a proxy endpoint, use the RDS API [CreateProxyEndpoint](#) action.

Viewing proxy endpoints

Console

To view the details for a proxy endpoint

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. In the list, choose the proxy whose endpoint you want to view. Click the proxy name to view its details page.
4. In the **Proxy endpoints** section, choose the endpoint that you want to view. Click its name to view the details page.
5. Examine the parameters whose values you're interested in. You can check properties such as the following:
 - Whether the endpoint is read/write or read-only.
 - The endpoint address that you use in a database connection string.
 - The VPC, subnets, and security groups associated with the endpoint.

AWS CLI

To view one or more DB proxy endpoints, use the AWS CLI [describe-db-proxy-endpoints](#) command.

You can include the following optional parameters:

- `--db-proxy-endpoint-name`
- `--db-proxy-name`

The following example describes the `my-endpoint` proxy endpoint.

Example

For Linux, macOS, or Unix:

```
aws rds describe-db-proxy-endpoints \
--db-proxy-endpoint-name my-endpoint
```

For Windows:

```
aws rds describe-db-proxy-endpoints ^
--db-proxy-endpoint-name my-endpoint
```

RDS API

To describe one or more proxy endpoints, use the RDS API [DescribeDBProxyEndpoints](#) operation.

Modifying a proxy endpoint

Console

To modify one or more proxy endpoints

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Proxies**.
3. In the list, choose the proxy whose endpoint you want to modify. Click the proxy name to view its details page.
4. In the **Proxy endpoints** section, choose the endpoint that you want to modify. You can select it in the list, or click its name to view the details page.
5. On the proxy details page, under the **Proxy endpoints** section, choose **Edit**. Or on the proxy endpoint details page, for **Actions**, choose **Edit**.
6. Change the values of the parameters that you want to modify.
7. Choose **Save changes**.

AWS CLI

To modify a DB proxy endpoint, use the AWS CLI [modify-db-proxy-endpoint](#) command with the following required parameters:

- `--db-proxy-endpoint-name`

Specify changes to the endpoint properties by using one or more of the following parameters:

- `--new-db-proxy-endpoint-name`
- `--vpc-security-group-ids`. Separate the security group IDs with spaces.

The following example renames the `my-endpoint` proxy endpoint to `new-endpoint-name`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-proxy-endpoint \
--db-proxy-endpoint-name my-endpoint \
--new-db-proxy-endpoint-name new-endpoint-name
```

For Windows:

```
aws rds modify-db-proxy-endpoint ^
--db-proxy-endpoint-name my-endpoint ^
--new-db-proxy-endpoint-name new-endpoint-name
```

RDS API

To modify a proxy endpoint, use the RDS API [ModifyDBProxyEndpoint](#) operation.

Deleting a proxy endpoint

You can delete an endpoint for your proxy using the console as described following.

Note

You can't delete the default endpoint that RDS Proxy automatically creates for each proxy.
When you delete a proxy, RDS Proxy automatically deletes all the associated endpoints.

Console

To delete a proxy endpoint using the AWS Management Console

1. In the navigation pane, choose **Proxies**.
2. In the list, choose the proxy whose endpoint you want to endpoint. Click the proxy name to view its details page.
3. In the **Proxy endpoints** section, choose the endpoint that you want to delete. You can select one or more endpoints in the list, or click the name of a single endpoint to view the details page.
4. On the proxy details page, under the **Proxy endpoints** section, choose **Delete**. Or on the proxy endpoint details page, for **Actions**, choose **Delete**.

AWS CLI

To delete a proxy endpoint, run the `delete-db-proxy-endpoint` command with the following required parameters:

- `--db-proxy-endpoint-name`

The following command deletes the proxy endpoint named `my-endpoint`.

For Linux, macOS, or Unix:

```
aws rds delete-db-proxy-endpoint \
--db-proxy-endpoint-name my-endpoint
```

For Windows:

```
aws rds delete-db-proxy-endpoint ^
--db-proxy-endpoint-name my-endpoint
```

RDS API

To delete a proxy endpoint with the RDS API, run the [DeleteDBProxyEndpoint](#) operation. Specify the name of the proxy endpoint for the DBProxyEndpointName parameter.

Limitations for proxy endpoints

Each proxy has a default endpoint that you can modify but not create or delete.

The maximum number of user-defined endpoints for a proxy is 20. Thus, a proxy can have up to 21 endpoints: the default endpoint, plus 20 that you create.

When you associate additional endpoints with a proxy, RDS Proxy automatically determines which DB instances in your cluster to use for each endpoint. You can't choose specific instances the way that you can with Aurora custom endpoints.

Reader endpoints aren't available for Aurora multi-writer clusters.

Monitoring RDS Proxy metrics with Amazon CloudWatch

You can monitor RDS Proxy by using Amazon CloudWatch. CloudWatch collects and processes raw data from the proxies into readable, near-real-time metrics. To find these metrics in the CloudWatch console, choose **Metrics**, then choose **RDS**, and choose **Per-Proxy Metrics**. For more information, see [Using Amazon CloudWatch metrics](#) in the Amazon CloudWatch User Guide.

Note

RDS publishes these metrics for each underlying Amazon EC2 instance associated with a proxy. A single proxy might be served by more than one EC2 instance. Use CloudWatch statistics to aggregate the values for a proxy across all the associated instances.

Some of these metrics might not be visible until after the first successful connection by a proxy.

In the RDS Proxy logs, each entry is prefixed with the name of the associated proxy endpoint. This name can be the name you specified for a user-defined endpoint, or the special name `default` for read/write requests using the default endpoint of a proxy.

All RDS Proxy metrics are in the group `proxy`.

Each proxy endpoint has its own CloudWatch metrics. You can monitor the usage of each proxy endpoint independently. For more information about proxy endpoints, see [Working with Amazon RDS Proxy endpoints \(p. 952\)](#).

You can aggregate the values for each metric using one of the following dimension sets. For example, by using the `ProxyName` dimension set, you can analyze all the traffic for a particular proxy. By using the other dimension sets, you can split the metrics in different ways. You can split the metrics based on

the different endpoints or target databases of each proxy, or the read/write and read-only traffic to each database.

- Dimension set 1: ProxyName
- Dimension set 2: ProxyName, EndpointName
- Dimension set 3: ProxyName, TargetGroup, Target
- Dimension set 4: ProxyName, TargetGroup, TargetRole

Metric	Description	Valid period	CloudWatch dimension set
AvailabilityPercentage	The percentage of time for which the target group was available in the role indicated by the dimension. This metric is reported every minute. The most useful statistic for this metric is Average.	1 minute	Dimension set 4 (p. 960)
ClientConnections	The current number of client connections. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
ClientConnectionsClosed	The number of client connections closed. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
ClientConnectionsNotEstablished	The current number of client connections without Transport Layer Security (TLS). This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
ClientConnectionsReceived	The number of client connection requests received. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
ClientConnectionsRejected	The number of client connection attempts that failed due to misconfigured authentication or TLS. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)

Metric	Description	Valid period	CloudWatch dimension set
ClientConnectionsSet	The number of client connections successfully established with any authentication mechanism with or without TLS. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
ClientConnectionsTLS	The current number of client connections with TLS. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
DatabaseConnectionRequests	The number of requests to create a database connection. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnectionRequestsTLS	The number of requests to create a database connection with TLS. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnections	The current number of database connections. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnectionsBorrowLatency	The total latency microseconds that it takes for the proxy being monitored to get a database connection. The most useful statistic for this metric is Average.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
DatabaseConnectionsBorrowed	The current number of database connections in the borrow state. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)

Metric	Description	Valid period	CloudWatch dimension set
DatabaseConnections	The current number of database connections in a transaction. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnections	The current session of database connections currently pinned because of operations in client requests that change session state. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnections	The number of database connection requests that failed. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnections	The number of database connections successfully established with or without TLS. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
DatabaseConnections	The current number of database connections with TLS. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
MaxDatabaseConnections	The allowed number of database connections allowed. This metric is reported every minute. The most useful statistic for this metric is Sum.	1 minute	Dimension set 1 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)

Metric	Description	Valid period	CloudWatch dimension set
QueryDatabaseResponseLatency	The time in microseconds that the database took to respond to the query. The most useful statistic for this metric is Average.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960) , Dimension set 3 (p. 960) , Dimension set 4 (p. 960)
QueryRequests	The number of queries received. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
QueryRequestsNoTLS	The number of queries received from non-TLS connections. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
QueryRequestsTLS	The number of queries received from TLS connections. A query including multiple statements is counted as one query. The most useful statistic for this metric is Sum.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)
QueryResponseLatency	The time in microseconds between getting a query request and the proxy responding to it. The most useful statistic for this metric is Average.	1 minute and above	Dimension set 1 (p. 960) , Dimension set 2 (p. 960)

You can find logs of RDS Proxy activity under CloudWatch in the AWS Management Console. Each proxy has an entry in the [Log groups](#) page.

Important

These logs are intended for human consumption for troubleshooting purposes and not for programmatic access. The format and content of the logs is subject to change.

In particular, older logs don't contain any prefixes indicating the endpoint for each request. In newer logs, each entry is prefixed with the name of the associated proxy endpoint. This name can be the name that you specified for a user-defined endpoint, or the special name default for requests using the default endpoint of a proxy.

Working with RDS Proxy events

An *event* indicates a change in an environment. This can be an AWS environment or a service or application from a software as a service (SaaS) partner. Or it can be one of your own custom applications or services. For example, Amazon RDS generates an event when you create or modify an RDS Proxy. Amazon RDS delivers events to CloudWatch Events and Amazon EventBridge in near-real time. Following, you can find a list of RDS Proxy events that you can subscribe to and an example of an RDS Proxy event.

For more information about working with events, see the following:

- For instructions on how to view events by using the AWS Management Console, AWS CLI, or RDS API, see [Viewing Amazon RDS events \(p. 647\)](#).
- To learn how to configure Amazon RDS to send events to EventBridge, see [Creating a rule that triggers on an Amazon RDS event \(p. 664\)](#).

RDS Proxy events

The following table shows the event category and a list of events when an RDS Proxy is the source type.

Category	RDS event ID	Description
configuration change	RDS-EVENT-0204	RDS modified the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0207	RDS modified the endpoint of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0213	RDS detected the addition of the DB instance and automatically added it to the target group of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0214	RDS detected the deletion of the DB instance and automatically removed it from the target group of the DB proxy (RDS Proxy).
configuration change	RDS-EVENT-0215	RDS detected the deletion of the DB cluster and automatically removed it from the target group of the DB proxy (RDS Proxy).
creation	RDS-EVENT-0203	RDS created the DB proxy (RDS Proxy).
creation	RDS-EVENT-0206	RDS created the endpoint for the DB proxy (RDS Proxy).
deletion	RDS-EVENT-0205	RDS deleted the DB proxy (RDS Proxy).
deletion	RDS-EVENT-0208	RDS deleted the endpoint of DB proxy (RDS Proxy).
failure	RDS-EVENT-0243	RDS couldn't provision capacity for the proxy because there aren't enough IP addresses available in your subnets. To fix the issue, make sure that your subnets have the minimum number of unused IP addresses. To determine the recommended number for your instance class, see Planning for IP address capacity (p. 930) .

The following is an example of an RDS Proxy event in JSON format. The event shows that RDS modified the endpoint named `my-endpoint` of the RDS Proxy named `my-rds-proxy`. The event ID is `RDS-EVENT-0207`.

```
{  
    "version": "0",  
    "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ffd4e",  
    "detail-type": "RDS DB Proxy Event",  
    "source": "aws.rds",  
    "account": "123456789012",  
    "time": "2018-09-27T22:36:43Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy"  
    ],  
    "detail": {  
        "EventCategories": [  
            "configuration change"  
        ],  
        "SourceType": "DB_PROXY",  
        "SourceArn": "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy",  
        "Date": "2018-09-27T22:36:43.292Z",  
        "Message": "RDS modified endpoint my-endpoint of DB Proxy my-rds-proxy.",  
        "SourceIdentifier": "my-endpoint",  
        "EventID": "RDS-EVENT-0207"  
    }  
}
```

RDS Proxy command-line examples

To see how combinations of connection commands and SQL statements interact with RDS Proxy, look at the following examples.

Examples

- [Preserving Connections to a MySQL Database Across a Failover](#)
- [Adjusting the max_connections Setting for an Aurora DB Cluster](#)

Example Preserving connections to a MySQL database across a failover

This MySQL example demonstrates how open connections continue working during a failover. An example is when you reboot a database or it becomes unavailable due to a problem. This example uses a proxy named `the-proxy` and an Aurora DB cluster with DB instances `instance-8898` and `instance-9814`. When you run the `failover-db-cluster` command from the Linux command line, the writer instance that the proxy is connected to changes to a different DB instance. You can see that the DB instance associated with the proxy changes while the connection remains open.

```
$ mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p  
Enter password:  
...  
  
mysql> select @@aurora_server_id;  
+-----+  
| @@aurora_server_id |  
+-----+  
| instance-9814 |  
+-----+
```

```

1 row in set (0.01 sec)

mysql>
[1]+ Stopped                  mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -
u admin_user -p
$ # Initially, instance-9814 is the writer.
$ aws rds failover-db-cluster --db-cluster-identifier cluster-56-2019-11-14-1399
JSON output
$ # After a short time, the console shows that the failover operation is complete.
$ # Now instance-8898 is the writer.
$ fg
mysql -h the-proxy.proxy-demo.us.us-east-1.rds.amazonaws.com -u admin_user -p

mysql> select @@aurora_server_id;
+-----+
| @@aurora_server_id |
+-----+
| instance-8898      |
+-----+
1 row in set (0.01 sec)

mysql>
[1]+ Stopped                  mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -
u admin_user -p
$ aws rds failover-db-cluster --db-cluster-identifier cluster-56-2019-11-14-1399
JSON output
$ # After a short time, the console shows that the failover operation is complete.
$ # Now instance-9814 is the writer again.
$ fg
mysql -h the-proxy.proxy-demo.us-east-1.rds.amazonaws.com -u admin_user -p

mysql> select @@aurora_server_id;
+-----+
| @@aurora_server_id |
+-----+
| instance-9814      |
+-----+
1 row in set (0.01 sec)
+-----+-----+
| Variable_name | Value      |
+-----+-----+
| hostname     | ip-10-1-3-178 |
+-----+-----+
1 row in set (0.02 sec)

```

Example Adjusting the max_connections setting for an Aurora DB cluster

This example demonstrates how you can adjust the max_connections setting for an Aurora MySQL DB cluster. To do so, you create your own DB cluster parameter group based on the default parameter settings for clusters that are compatible with MySQL 5.6 or 5.7. You specify a value for the max_connections setting, overriding the formula that sets the default value. You associate the DB cluster parameter group with your DB cluster.

```

export REGION=us-east-1
export CLUSTER_PARAM_GROUP=rds-proxy-mysql-56-max-connections-demo
export CLUSTER_NAME=rds-proxy-mysql-56

aws rds create-db-parameter-group --region $REGION \
    --db-parameter-group-family aurora5.6 \
    --db-parameter-group-name $CLUSTER_PARAM_GROUP \
    --description "Aurora MySQL 5.6 cluster parameter group for RDS Proxy demo."

aws rds modify-db-cluster --region $REGION \
    --db-cluster-identifier $CLUSTER_NAME \

```

```
--db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP

echo "New cluster param group is assigned to cluster:"
aws rds describe-db-clusters --region $REGION \
--db-cluster-identifier $CLUSTER_NAME \
--query '*[*].{DBClusterParameterGroup:DBClusterParameterGroup}'

echo "Current value for max_connections:"
aws rds describe-db-cluster-parameters --region $REGION \
--db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP \
--query '*[*].{ParameterName:ParameterName,ParameterValue:ParameterValue}' \
--output text | grep "max_connections"

echo -n "Enter number for max_connections setting: "
read answer

aws rds modify-db-cluster-parameter-group --region $REGION --db-cluster-parameter-group-
name $CLUSTER_PARAM_GROUP \
--parameters "ParameterName=max_connections,ParameterValue=$
$answer,ApplyMethod=immediate"

echo "Updated value for max_connections:"
aws rds describe-db-cluster-parameters --region $REGION \
--db-cluster-parameter-group-name $CLUSTER_PARAM_GROUP \
--query '*[*].{ParameterName:ParameterName,ParameterValue:ParameterValue}' \
--output text | grep "max_connections"
```

Troubleshooting for RDS Proxy

Following, you can find troubleshooting ideas for some common RDS Proxy issues and information on CloudWatch logs for RDS Proxy.

In the RDS Proxy logs, each entry is prefixed with the name of the associated proxy endpoint. This name can be the name that you specified for a user-defined endpoint. Or it can be the special name default for read/write requests using the default endpoint of a proxy. For more information about proxy endpoints, see [Working with Amazon RDS Proxy endpoints \(p. 952\)](#).

Topics

- [Verifying connectivity for a proxy \(p. 967\)](#)
- [Common issues and solutions \(p. 968\)](#)

Verifying connectivity for a proxy

You can use the following commands to verify that all components of the connection mechanism can communicate with the other components.

Examine the proxy itself using the [describe-db-proxies](#) command. Also examine the associated target group using the [describe-db-proxy-target-groups](#) command. Check that the details of the targets match the RDS DB instance or Aurora DB cluster that you intend to associate with the proxy. Use commands such as the following.

```
aws rds describe-db-proxies --db-proxy-name $DB_PROXY_NAME
aws rds describe-db-proxy-target-groups --db-proxy-name $DB_PROXY_NAME
```

To confirm that the proxy can connect to the underlying database, examine the targets specified in the target groups using the [describe-db-proxy-targets](#) command. Use a command such as the following.

```
aws rds describe-db-proxy-targets --db-proxy-name $DB_PROXY_NAME
```

The output of the [describe-db-proxy-targets](#) command includes a TargetHealth field. You can examine the fields State, Reason, and Description inside TargetHealth to check if the proxy can communicate with the underlying DB instance.

- A State value of AVAILABLE indicates that the proxy can connect to the DB instance.
- A State value of UNAVAILABLE indicates a temporary or permanent connection problem. In this case, examine the Reason and Description fields. For example, if Reason has a value of PENDING_PROXY_CAPACITY, try connecting again after the proxy finishes its scaling operation. If Reason has a value of UNREACHABLE, CONNECTION_FAILED, or AUTH_FAILURE, use the explanation from the Description field to help you diagnose the issue.
- The State field might have a value of REGISTERING for a brief time before changing to AVAILABLE or UNAVAILABLE.

If the following Netcat command (nc) is successful, you can access the proxy endpoint from the EC2 instance or other system where you're logged in. This command reports failure if you're not in the same VPC as the proxy and the associated database. You might be able to log directly in to the database without being in the same VPC. However, you can't log into the proxy unless you're in the same VPC.

```
nc -zx MySQL_proxy_endpoint 3306  
nc -zx PostgreSQL_proxy_endpoint 5432
```

You can use the following commands to make sure that your EC2 instance has the required properties. In particular, the VPC for the EC2 instance must be the same as the VPC for the RDS DB instance or Aurora DB cluster that the proxy connects to.

```
aws ec2 describe-instances --instance-ids your_ec2_instance_id
```

Examine the Secrets Manager secrets used for the proxy.

```
aws secretsmanager list-secrets  
aws secretsmanager get-secret-value --secret-id your_secret_id
```

Make sure that the SecretString field displayed by get-secret-value is encoded as a JSON string that includes username and password fields. The following example shows the format of the SecretString field.

```
{  
    "ARN": "some_arn",  
    "Name": "some_name",  
    "VersionId": "some_version_id",  
    "SecretString": '{"username":"some_username","password":"some_password"}',  
    "VersionStages": [ "some_stage" ],  
    "CreatedDate": "some_timestamp"  
}
```

Common issues and solutions

For possible causes and solutions to some common problems that you might encounter using RDS Proxy, see the following.

You might encounter the following issues while creating a new proxy or connecting to a proxy.

Error	Causes or workarounds
403: The security token included in the request is invalid	Select an existing IAM role instead of choosing to create a new one.

You might encounter the following issues while connecting to a MySQL proxy.

Error	Causes or workarounds
ERROR 1040 (HY000): Connections rate limit exceeded (<i>limit_value</i>)	The rate of connection requests from the client to the proxy has exceeded the limit.
ERROR 1040 (HY000): IAM authentication rate limit exceeded	The number of simultaneous requests with IAM authentication from the client to the proxy has exceeded the limit.
ERROR 1040 (HY000): Number simultaneous connections exceeded (<i>limit_value</i>)	The number of simultaneous connection requests from the client to the proxy exceeded the limit.
ERROR 1045 (28000): Access denied for user ' <i>DB_USER</i> '@'%' (using password: YES)	Some possible reasons include the following: <ul style="list-style-type: none"> The Secrets Manager secret used by the proxy doesn't match the user name and password of an existing database user. Either update the credentials in the Secrets Manager secret, or make sure the database user exists and has the same password as in the secret.
ERROR 1105 (HY000): Unknown error	An unknown error occurred.
ERROR 1231 (42000): Variable 'character_set_client' can't be set to the value of <i>value</i>	The value set for the character_set_client parameter is not valid. For example, the value ucs2 is not valid because it can crash the MySQL server.
ERROR 3159 (HY000): This RDS Proxy requires TLS connections.	You enabled the setting Require Transport Layer Security in the proxy but your connection included the parameter ssl-mode=DISABLED in the MySQL client. Do either of the following: <ul style="list-style-type: none"> Disable the setting Require Transport Layer Security for the proxy. Connect to the database using the minimum setting of ssl-mode=REQUIRED in the MySQL client.

Error	Causes or workarounds
ERROR 2026 (HY000): SSL connection error: Internal Server Error	<p>The TLS handshake to the proxy failed. Some possible reasons include the following:</p> <ul style="list-style-type: none"> SSL is required but the server doesn't support it. An internal server error occurred. A bad handshake occurred.
ERROR 9501 (HY000): Timed-out waiting to acquire database connection	<p>The proxy timed-out waiting to acquire a database connection. Some possible reasons include the following:</p> <ul style="list-style-type: none"> The proxy is unable to establish a database connection because the maximum connections have been reached The proxy is unable to establish a database connection because the database is unavailable.

You might encounter the following issues while connecting to a PostgreSQL proxy.

Error	Cause	Solution
IAM authentication is allowed only with SSL connections.	The user tried to connect to the database using IAM authentication with the setting <code>sslmode=disable</code> in the PostgreSQL client.	The user needs to connect to the database using the minimum setting of <code>sslmode=require</code> in the PostgreSQL client. For more information, see the PostgreSQL SSL support documentation.
This RDS Proxy requires TLS connections.	The user enabled the option Require Transport Layer Security but tried to connect with <code>sslmode=disable</code> in the PostgreSQL client.	To fix this error, do one of the following: <ul style="list-style-type: none"> Disable the proxy's Require Transport Layer Security option. Connect to the database using the minimum setting of <code>sslmode=allow</code> in the PostgreSQL client.
IAM authentication failed for user <code>user_name</code> . Check the IAM token for this user and try again.	<p>This error might be due to the following reasons:</p> <ul style="list-style-type: none"> The client supplied the incorrect IAM user name. The client supplied an incorrect IAM authorization token for the user. The client is using an IAM policy that does not have the necessary permissions. The client supplied an expired IAM authorization token for the user. 	To fix this error, do the following: <ol style="list-style-type: none"> Confirm that the provided IAM user exists. Confirm that the IAM authorization token belongs to the provided IAM user. Confirm that the IAM policy has adequate permissions for RDS. Check the validity of the IAM authorization token used.

Error	Cause	Solution
This RDS proxy has no credentials for the role <i>role_name</i> . Check the credentials for this role and try again.	There is no Secrets Manager secret for this role.	Add a Secrets Manager secret for this role.
RDS supports only IAM or MD5 authentication.	The database client being used to connect to the proxy is using an authentication mechanism not currently supported by the proxy, such as SCRAM-SHA-256.	If you're not using IAM authentication, use the MD5 password authentication only.
A user name is missing from the connection startup packet. Provide a user name for this connection.	The database client being used to connect to the proxy isn't sending a user name when trying to establish a connection.	Make sure to define a user name when setting up a connection to the proxy using the PostgreSQL client of your choice.
Feature not supported: RDS Proxy supports only version 3.0 of the PostgreSQL messaging protocol.	The PostgreSQL client used to connect to the proxy uses a protocol older than 3.0.	Use a newer PostgreSQL client that supports the 3.0 messaging protocol. If you're using the PostgreSQL psql CLI, use a version greater than or equal to 7.4.
Feature not supported: RDS Proxy currently doesn't support streaming replication mode.	The PostgreSQL client used to connect to the proxy is trying to use the streaming replication mode, which isn't currently supported by RDS Proxy.	Turn off the streaming replication mode in the PostgreSQL client being used to connect.
Feature not supported: RDS Proxy currently doesn't support the option <i>option_name</i> .	Through the startup message, the PostgreSQL client used to connect to the proxy is requesting an option that isn't currently supported by RDS Proxy.	Turn off the option being shown as not supported from the message above in the PostgreSQL client being used to connect.
The IAM authentication failed because of too many competing requests.	The number of simultaneous requests with IAM authentication from the client to the proxy has exceeded the limit.	Reduce the rate in which connections using IAM authentication from a PostgreSQL client are established.
The maximum number of client connections to the proxy exceeded <i>number_value</i> .	The number of simultaneous connection requests from the client to the proxy exceeded the limit.	Reduce the number of active connections from PostgreSQL clients to this RDS proxy.
Rate of connection to proxy exceeded <i>number_value</i> .	The rate of connection requests from the client to the proxy has exceeded the limit.	Reduce the rate in which connections from a PostgreSQL client are established.

Error	Cause	Solution
The password that was provided for the role <i>role_name</i> is wrong.	The password for this role doesn't match the Secrets Manager secret.	Check the secret for this role in Secrets Manager to see if the password is the same as what's being used in your PostgreSQL client.
The IAM authentication failed for the role <i>role_name</i> . Check the IAM token for this role and try again.	There is a problem with the IAM token used for IAM authentication.	Generate a new authentication token and use it in a new connection.
IAM is allowed only with SSL connections.	A client tried to connect using IAM authentication, but SSL wasn't enabled.	Enable SSL in the PostgreSQL client.
Unknown error.	An unknown error occurred.	Reach out to AWS Support to investigate the issue.
Timed-out waiting to acquire database connection.	<p>The proxy timed-out waiting to acquire a database connection. Some possible reasons include the following:</p> <ul style="list-style-type: none"> The proxy can't establish a database connection because the maximum connections have been reached. The proxy can't establish a database connection because the database is unavailable. 	<p>Possible solutions are the following:</p> <ul style="list-style-type: none"> Check the target of the RDS DB instance or Aurora DB cluster status to see if it's unavailable. Check if there are long-running transactions and/or queries being executed. They can use database connections from the connection pool for a long time.
Request returned an error: <i>database_error</i> .	The database connection established from the proxy returned an error.	The solution depends on the specific database error. One example is: Request returned an error: database "your-database-name" does not exist. This means that the specified database name doesn't exist on the database server. Or it means that the user name used as a database name (if a database name isn't specified) doesn't exist on the server.

Using RDS Proxy with AWS CloudFormation

You can use RDS Proxy with AWS CloudFormation. Doing so helps you to create groups of related resources. Such a group can include a proxy that can connect to a newly created Amazon RDS DB instance or Aurora DB cluster. RDS Proxy support in AWS CloudFormation involves two new registry types: `DBProxy` and `DBProxyTargetGroup`.

The following listing shows a sample AWS CloudFormation template for RDS Proxy.

```
Resources:
  DBProxy:
    Type: AWS::RDS::DBProxy
    Properties:
      DBProxyName: CanaryProxy
      EngineFamily: MYSQL
      RoleArn:
        Fn::ImportValue: SecretReaderRoleArn
      Auth:
        - {AuthScheme: SECRETS, SecretArn: !ImportValue ProxySecret, IAMAuth: DISABLED}
      VpcSubnetIds:
        Fn::Split: [",", "Fn::ImportValue": SubnetIds]

  ProxyTargetGroup:
    Type: AWS::RDS::DBProxyTargetGroup
    Properties:
      DBProxyName: CanaryProxy
      TargetGroupName: default
      DBInstanceIdentifiers:
        - Fn::ImportValue: DBInstanceName
    DependsOn: DBProxy
```

For more information about the Amazon RDS and Aurora resources that you can create using AWS CloudFormation, see [RDS resource type reference](#).

Amazon RDS for MariaDB

Amazon RDS supports DB instances that run the following versions of MariaDB:

- MariaDB 10.6
- MariaDB 10.5
- MariaDB 10.4
- MariaDB 10.3
- MariaDB 10.2 (end of life scheduled for October 15, 2022)

For more information about minor version support, see [MariaDB on Amazon RDS versions \(p. 982\)](#).

To create a MariaDB DB instance, use the Amazon RDS management tools or interfaces. You can then use the Amazon RDS tools to perform management actions for the DB instance. These include actions such as the following:

- Reconfiguring or resizing the DB instance
- Authorizing connections to the DB instance
- Creating and restoring from backups or snapshots
- Creating Multi-AZ secondaries
- Creating read replicas
- Monitoring the performance of your DB instance

To store and access the data in your DB instance, use standard MariaDB utilities and applications.

MariaDB is available in all of the AWS Regions. For more information about AWS Regions, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

You can use Amazon RDS for MariaDB databases to build HIPAA-compliant applications. You can store healthcare-related information, including protected health information (PHI), under a Business Associate Agreement (BAA) with AWS. For more information, see [HIPAA compliance](#). AWS Services in Scope have been fully assessed by a third-party auditor and result in a certification, attestation of compliance, or Authority to Operate (ATO). For more information, see [AWS services in scope by compliance program](#).

Before creating a DB instance, complete the steps in [Setting up for Amazon RDS \(p. 148\)](#). When you create a DB instance, the RDS master user gets DBA privileges, with some limitations. Use this account for administrative tasks such as creating additional database accounts.

You can create the following:

- DB instances
- DB snapshots
- Point-in-time restores
- Automated backups
- Manual backups

You can use DB instances running MariaDB inside a virtual private cloud (VPC) based on Amazon VPC. You can also add features to your MariaDB DB instance by enabling various options. Amazon RDS supports Multi-AZ deployments for MariaDB as a high-availability, failover solution.

Important

To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. It also restricts access to certain system procedures and tables that need advanced privileges. You can access your database using standard SQL clients such as the mysql client. However, you can't access the host directly by using Telnet or Secure Shell (SSH).

Topics

- [MariaDB feature support on Amazon RDS \(p. 975\)](#)
- [MariaDB on Amazon RDS versions \(p. 982\)](#)
- [Connecting to a DB instance running the MariaDB database engine \(p. 986\)](#)
- [Securing MariaDB DB instance connections \(p. 991\)](#)
- [Upgrading the MariaDB DB engine \(p. 998\)](#)
- [Importing data into a MariaDB DB instance \(p. 1003\)](#)
- [Working with MariaDB replication in Amazon RDS \(p. 1024\)](#)
- [Options for MariaDB database engine \(p. 1040\)](#)
- [Parameters for MariaDB \(p. 1043\)](#)
- [Migrating data from a MySQL DB snapshot to a MariaDB DB instance \(p. 1046\)](#)
- [MariaDB on Amazon RDS SQL reference \(p. 1049\)](#)
- [Local time zone for MariaDB DB instances \(p. 1054\)](#)
- [RDS for MariaDB limitations \(p. 1056\)](#)

MariaDB feature support on Amazon RDS

RDS for MariaDB supports most of the features and capabilities of MariaDB. Some features might have limited support or restricted privileges.

You can filter new Amazon RDS features on the [What's New with Database?](#) page. For **Products**, choose **Amazon RDS**. Then search using keywords such as **MariaDB 2022**.

Note

The following lists are not exhaustive.

Topics

- [MariaDB feature support on Amazon RDS for MariaDB major versions \(p. 975\)](#)
- [Supported storage engines for MariaDB on Amazon RDS \(p. 979\)](#)
- [Cache warming for MariaDB on Amazon RDS \(p. 980\)](#)
- [MariaDB features not supported by Amazon RDS \(p. 981\)](#)

MariaDB feature support on Amazon RDS for MariaDB major versions

In the following sections, find information about MariaDB feature support on Amazon RDS for MariaDB major versions:

Topics

- [MariaDB 10.6 support on Amazon RDS \(p. 976\)](#)
- [MariaDB 10.5 support on Amazon RDS \(p. 977\)](#)
- [MariaDB 10.4 support on Amazon RDS \(p. 977\)](#)
- [MariaDB 10.3 support on Amazon RDS \(p. 978\)](#)

- [MariaDB 10.2 support on Amazon RDS \(p. 978\)](#)

For information about supported minor versions of Amazon RDS for MariaDB, see [MariaDB on Amazon RDS versions \(p. 982\)](#).

MariaDB 10.6 support on Amazon RDS

Amazon RDS supports the following new features for your DB instances running MariaDB version 10.6 or higher:

- **MyRocks storage engine** – You can use the MyRocks storage engine with RDS for MariaDB to optimize storage consumption of your write-intensive, high-performance web applications. For more information, see [Supported storage engines for MariaDB on Amazon RDS \(p. 979\)](#) and [MyRocks](#).
- **AWS Identity and Access Management (IAM) DB authentication** – You can use IAM DB authentication for better security and central management of connections to your MariaDB DB instances. For more information, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).
- **Upgrade options** – You can now upgrade to RDS for MariaDB version 10.6 from any prior major release (10.2, 10.3, 10.4, 10.5). You can also restore a snapshot of an existing MySQL 5.6 or 5.7 DB instance to a MariaDB 10.6 instance. For more information, see [Upgrading the MariaDB DB engine \(p. 998\)](#).
- **Delayed replication** – You can now set a configurable time period for which a read replica lags behind the source database. In a standard MariaDB replication configuration, there is minimal replication delay between the source and the replica. With delayed replication, you can set an intentional delay as a strategy for disaster recovery. For more information, see [Configuring delayed replication with MariaDB \(p. 1030\)](#).
- **Oracle PL/SQL compatibility** – By using RDS for MariaDB version 10.6, you can more easily migrate your legacy Oracle applications to Amazon RDS. For more information, see [SQL_MODE=ORACLE](#).
- **Atomic DDL** – Your dynamic data language (DDL) statements can be relatively crash-safe with RDS for MariaDB version 10.6. CREATE TABLE, ALTER TABLE, RENAME TABLE, DROP TABLE, DROP DATABASE and related DDL statements are now atomic. Either the statement succeeds, or it's completely reversed. For more information, see [Atomic DDL](#).
- **Other enhancements** – These enhancements include a JSON_TABLE function for transforming JSON data to relational format within SQL, and faster empty table data load with Innodb. They also include new sys_schema for analysis and troubleshooting, optimizer enhancement for ignoring unused indexes, and performance improvements. For more information, see [JSON_TABLE](#).
- **New default values for parameters** – The following parameters have new default values for MariaDB version 10.6 DB instances:
 - The default value for the following parameters has changed from utf8 to utf8mb3:
 - [character_set_client](#)
 - [character_set_connection](#)
 - [character_set_results](#)
 - [character_set_system](#)

Although the default values have changed for these parameters, there is no functional change. For more information, see [Supported Character Sets and Collations](#) in the MariaDB documentation.

- The default value of the [collation_connection](#) parameter has changed from utf8_general_ci to utf8mb3_general_ci. Although the default value has changed for this parameter, there is no functional change.
- The default value of the [old_mode](#) parameter has changed from unset to UTF8_IS_UTF8MB3. Although the default value has changed for this parameter, there is no functional change.

For a list of all MariaDB 10.6 features and their documentation, see [Changes and improvements in MariaDB 10.6](#) and [Release notes - MariaDB 10.6 series](#) on the MariaDB website.

For a list of unsupported features, see [MariaDB features not supported by Amazon RDS \(p. 981\)](#).

MariaDB 10.5 support on Amazon RDS

Amazon RDS supports the following new features for your DB instances running MariaDB version 10.5 or later:

- **InnoDB enhancements** – MariaDB version 10.5 includes InnoDB enhancements. For more information, see [InnoDB: Performance Improvements etc.](#) in the MariaDB documentation.
- **Performance schema updates** – MariaDB version 10.5 includes performance schema updates. For more information, see [Performance Schema Updates to Match MySQL 5.7 Instrumentation and Tables](#) in the MariaDB documentation.
- **One file in the InnoDB redo log** – In versions of MariaDB before version 10.5, the value of the `innodb_log_files_in_group` parameter was set to 2. In MariaDB version 10.5, the value of this parameter is set to 1.

If you are upgrading from a prior version to MariaDB version 10.5, and you don't modify the parameters, the `innodb_log_file_size` parameter value is unchanged. However, it applies to one log file instead of two. The result is that your upgraded MariaDB version 10.5 DB instance uses half of the redo log size that it was using before the upgrade. This change can have a noticeable performance impact. To address this issue, you can double the value of the `innodb_log_file_size` parameter. For information about modifying parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

- **SHOW SLAVE STATUS command not supported** – In versions of MariaDB before version 10.5, the `SHOW SLAVE STATUS` command required the `REPLICATION SLAVE` privilege. In MariaDB version 10.5, the equivalent `SHOW REPLICA STATUS` command requires the `REPLICATION REPLICA ADMIN` privilege. This new privilege isn't granted to the RDS master user.

Instead of using the `SHOW REPLICA STATUS` command, run the new `mysql.rds_replica_status` stored procedure to return similar information. For more information, see [mysql.rds_replica_status \(p. 1049\)](#).

- **SHOW RELAYLOG EVENTS command not supported** – In versions of MariaDB before version 10.5, the `SHOW RELAYLOG EVENTS` command required the `REPLICATION SLAVE` privilege. In MariaDB version 10.5, this command requires the `REPLICATION REPLICA ADMIN` privilege. This new privilege isn't granted to the RDS master user.
- **New default values for parameters** – The following parameters have new default values for MariaDB version 10.5 DB instances:
 - The default value of the `max_connections` parameter has changed to `LEAST({DBInstanceClassMemory/25165760}, 12000)`. For information about the `LEAST` parameter function, see [DB parameter functions \(p. 312\)](#).
 - The default value of the `innodb_adaptive_hash_index` parameter has changed to `OFF (0)`.
 - The default value of the `innodb_checksum_algorithm` parameter has changed to `full_crc32`.
 - The default value of the `innodb_log_file_size` parameter has changed to 2 GB.

For a list of all MariaDB 10.5 features and their documentation, see [Changes and improvements in MariaDB 10.5](#) and [Release notes - MariaDB 10.5 series](#) on the MariaDB website.

For a list of unsupported features, see [MariaDB features not supported by Amazon RDS \(p. 981\)](#).

MariaDB 10.4 support on Amazon RDS

Amazon RDS supports the following new features for your DB instances running MariaDB version 10.4 or later:

- **User account security enhancements** – Password expiration and [account locking improvements](#)

- **Optimizer enhancements** – Optimizer trace feature
- **InnoDB enhancements** – Instant DROP COLUMN support and instant VARCHAR extension for ROW_FORMAT=DYNAMIC and ROW_FORMAT=COMPACT
- **New parameters** – Including `tcp_nodedelay`, `tls_version`, and `gtid_cleanup_batch_size`

For a list of all MariaDB 10.4 features and their documentation, see [Changes and improvements in MariaDB 10.4](#) and [Release notes - MariaDB 10.4 series](#) on the MariaDB website.

For a list of unsupported features, see [MariaDB features not supported by Amazon RDS \(p. 981\)](#).

MariaDB 10.3 support on Amazon RDS

Amazon RDS supports the following new features for your DB instances running MariaDB version 10.3 or later:

- **Oracle compatibility** – PL/SQL compatibility parser, sequences, INTERSECT and EXCEPT to complement UNION, new TYPE OF and ROW TYPE OF declarations, and invisible columns
- **Temporal data processing** – System versioned tables for querying of past and present states of the database
- **Flexibility** – User-defined aggregates, storage-independent column compression, and proxy protocol support to relay the client IP address to the server
- **Manageability** – Instant ADD COLUMN operations and fast-fail data definition language (DDL) operations

For a list of all MariaDB 10.3 features and their documentation, see [Changes & improvements in MariaDB 10.3](#) and [Release notes - MariaDB 10.3 series](#) on the MariaDB website.

For a list of unsupported features, see [MariaDB features not supported by Amazon RDS \(p. 981\)](#).

MariaDB 10.2 support on Amazon RDS

Amazon RDS supports the following new features for your DB instances running MariaDB version 10.2 or later:

- ALTER USER
- Common Table Expressions
- Compressing Events to Reduce Size of the Binary Log
- CREATE USER — new options for limiting resource usage and SSL/TLS
- EXECUTE IMMEDIATE
- Flashback
- InnoDB — now the default storage engine instead of XtraDB
- InnoDB — set the buffer pool size dynamically
- JSON Functions
- Window Functions
- WITH

For a list of all MariaDB 10.2 features and their documentation, see [Changes & improvements in MariaDB 10.2](#) and [Release notes - MariaDB 10.2 series](#) on the MariaDB website.

For a list of unsupported features, see [MariaDB features not supported by Amazon RDS \(p. 981\)](#).

Supported storage engines for MariaDB on Amazon RDS

RDS for MariaDB supports the following storage engines.

Topics

- [The InnoDB storage engine \(p. 979\)](#)
- [The MyRocks storage engine \(p. 979\)](#)

Other storage engines aren't currently supported by RDS for MariaDB.

The InnoDB storage engine

Although MariaDB supports multiple storage engines with varying capabilities, not all of them are optimized for recovery and data durability. InnoDB is the recommended storage engine for MariaDB DB instances on Amazon RDS. Amazon RDS features such as point-in-time restore and snapshot restore require a recoverable storage engine and are supported only for the recommended storage engine for the MariaDB version.

For more information, see [InnoDB](#).

The MyRocks storage engine

The MyRocks storage engine is available in RDS for MariaDB version 10.6 and higher. Before using the MyRocks storage engine in a production database, we recommend that you perform thorough benchmarking and testing to verify any potential benefits over InnoDB for your use case.

The default parameter group for MariaDB version 10.6 includes MyRocks parameters. For more information, see [Parameters for MariaDB \(p. 1043\)](#) and [Working with parameter groups \(p. 289\)](#).

To create a table that uses the MyRocks storage engine, specify ENGINE= RocksDB in the CREATE TABLE statement. The following example creates a table that uses the MyRocks storage engine.

```
CREATE TABLE test (a INT NOT NULL, b CHAR(10)) ENGINE=RocksDB;
```

We strongly recommend that you don't run transactions that span both InnoDB and MyRocks tables. MariaDB doesn't guarantee ACID (atomicity, consistency, isolation, durability) for transactions across storage engines. Although it is possible to have both InnoDB and MyRocks tables in a DB instance, we don't recommend this approach except during a migration from one storage engine to the other. When both InnoDB and MyRocks tables exist in a DB instance, each storage engine has its own buffer pool, which might cause performance to degrade.

MyRocks doesn't support SERIALIZABLE isolation or gap locks. So, generally you can't use MyRocks with statement-based replication. For more information, see [MyRocks and Replication](#).

Currently, you can modify only the following MyRocks parameters:

- [rocksdb_block_cache_size](#)
- [rocksdb_bulk_load](#)
- [rocksdb_bulk_load_size](#)
- [rocksdb_deadlock_detect](#)
- [rocksdb_deadlock_detect_depth](#)

- [rocksdb_max_latest_deadlocks](#)

The MyRocks storage engine and the InnoDB storage engine can compete for memory based on the settings for the `rocksdb_block_cache_size` and `innodb_buffer_pool_size` parameters. In some cases, you might only intend to use the MyRocks storage engine on a particular DB instance. If so, we recommend setting the `innodb_buffer_pool_size` minimal parameter to a minimal value and setting the `rocksdb_block_cache_size` as high as possible.

You can access MyRocks log files by using the [DescribeDBLogFiles](#) and [DownloadDBLogFilePortion](#) operations.

For more information about MyRocks, see [MyRocks](#) on the MariaDB website.

Cache warming for MariaDB on Amazon RDS

InnoDB cache warming can provide performance gains for your MariaDB DB instance by saving the current state of the buffer pool when the DB instance is shut down, and then reloading the buffer pool from the saved information when the DB instance starts up. This approach bypasses the need for the buffer pool to "warm up" from normal database use and instead preloads the buffer pool with the pages for known common queries. For more information on cache warming, see [Dumping and restoring the buffer pool](#) in the MariaDB documentation.

Cache warming is enabled by default on MariaDB 10.2 and higher DB instances. To enable it, set the `innodb_buffer_pool_dump_at_shutdown` and `innodb_buffer_pool_load_at_startup` parameters to 1 in the parameter group for your DB instance. Changing these parameter values in a parameter group affects all MariaDB DB instances that use that parameter group. To enable cache warming for specific MariaDB DB instances, you might need to create a new parameter group for those DB instances. For information on parameter groups, see [Working with parameter groups \(p. 289\)](#).

Cache warming primarily provides a performance benefit for DB instances that use standard storage. If you use PIOPS storage, you don't commonly see a significant performance benefit.

Important

If your MariaDB DB instance doesn't shut down normally, such as during a failover, then the buffer pool state isn't saved to disk. In this case, MariaDB loads whatever buffer pool file is available when the DB instance is restarted. No harm is done, but the restored buffer pool might not reflect the most recent state of the buffer pool before the restart. To ensure that you have a recent state of the buffer pool available to warm the cache on startup, we recommend that you periodically dump the buffer pool "on demand." You can dump or load the buffer pool on demand.

You can create an event to dump the buffer pool automatically and at a regular interval. For example, the following statement creates an event named `periodic_buffer_pool_dump` that dumps the buffer pool every hour.

```
CREATE EVENT periodic_buffer_pool_dump
  ON SCHEDULE EVERY 1 HOUR
  DO CALL mysql.rds_innodb_buffer_pool_dump_now();
```

For more information, see [Events](#) in the MariaDB documentation.

Dumping and loading the buffer pool on demand

You can save and load the cache on demand using the following stored procedures:

- To dump the current state of the buffer pool to disk, call the [mysql.rds_innodb_buffer_pool_dump_now \(p. 1458\)](#) stored procedure.

- To load the saved state of the buffer pool from disk, call the [mysql.rds_innodb_buffer_pool_load_now \(p. 1458\)](#) stored procedure.
- To cancel a load operation in progress, call the [mysql.rds_innodb_buffer_pool_load_abort \(p. 1459\)](#) stored procedure.

MariaDB features not supported by Amazon RDS

The following MariaDB features are not supported on Amazon RDS:

- S3 storage engine
- Authentication plugin – GSSAPI
- Authentication plugin – Unix Socket
- AWS Key Management encryption plugin
- Delayed replication for MariaDB versions lower than 10.6
- Native MariaDB encryption at rest for InnoDB and Aria.

You can enable encryption at rest for a MariaDB DB instance by following the instructions in [Encrypting Amazon RDS resources \(p. 2000\)](#).

- HandlerSocket
- JSON table type for MariaDB versions lower than 10.6
- MariaDB ColumnStore
- MariaDB Galera Cluster
- Multisource replication
- MyRocks storage engine for MariaDB versions lower than 10.6
- Password validation plugin, `simple_password_check`, and `cracklib_password_check`
- Spider storage engine
- Sphinx storage engine
- TokuDB storage engine
- Storage engine-specific object attributes, as described in [Engine-defined new Table/Field/Index attributes](#) in the MariaDB documentation
- Table and tablespace encryption

To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges. Amazon RDS supports access to databases on a DB instance using any standard SQL client application. Amazon RDS doesn't allow direct host access to a DB instance by using Telnet, Secure Shell (SSH), or Windows Remote Desktop Connection.

MariaDB on Amazon RDS versions

For MariaDB, version numbers are organized as version X.Y.Z. In Amazon RDS terminology, X.Y denotes the major version, and Z is the minor version number. For Amazon RDS implementations, a version change is considered major if the major version number changes, for example going from version 10.5 to 10.6. A version change is considered minor if only the minor version number changes, for example going from version 10.6.5 to 10.6.7.

Topics

- [Supported MariaDB versions on Amazon RDS \(p. 982\)](#)
- [RDS for MariaDB release calendar \(p. 983\)](#)
- [MariaDB 10.3 end of life \(p. 984\)](#)
- [MariaDB 10.2 end of life \(p. 984\)](#)
- [Deprecated versions for Amazon RDS for MariaDB \(p. 985\)](#)

Supported MariaDB versions on Amazon RDS

Amazon RDS currently supports the following versions of MariaDB:

Major version	Minor version
MariaDB 10.6	<ul style="list-style-type: none">• 10.6.11• 10.6.10• 10.6.8• 10.6.7• 10.6.5
MariaDB 10.5	<ul style="list-style-type: none">• 10.5.18• 10.5.17• 10.5.16• 10.5.15• 10.5.13• 10.5.12
MariaDB 10.4	<ul style="list-style-type: none">• 10.4.27• 10.4.26• 10.4.25• 10.4.24
MariaDB 10.3	<ul style="list-style-type: none">• 10.3.37• 10.3.36• 10.3.35• 10.3.34

You can specify any currently supported MariaDB version when creating a new DB instance. You can specify the major version (such as MariaDB 10.5), and any supported minor version for the specified major version. If no version is specified, Amazon RDS defaults to a supported version, typically the most recent version. If a major version is specified but a minor version is not, Amazon RDS defaults to a recent

release of the major version you have specified. To see a list of supported versions, as well as defaults for newly created DB instances, use the [describe-db-engine-versions](#) AWS CLI command.

For example, to list the supported engine versions for RDS for MariaDB, run the following CLI command:

```
aws rds describe-db-engine-versions --engine mariadb --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

The default MariaDB version might vary by AWS Region. To create a DB instance with a specific minor version, specify the minor version during DB instance creation. You can determine the default minor version for an AWS Region using the following AWS CLI command:

```
aws rds describe-db-engine-versions --default-only --engine mariadb --engine-version major-engine-version --region region --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

Replace *major-engine-version* with the major engine version, and replace *region* with the AWS Region. For example, the following AWS CLI command returns the default MariaDB minor engine version for the 10.5 major version and the US West (Oregon) AWS Region (us-west-2):

```
aws rds describe-db-engine-versions --default-only --engine mariadb --engine-version 10.5 --region us-west-2 --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

RDS for MariaDB release calendar

RDS for MariaDB major versions remain available at least until community end of life for the corresponding community version. You can use the following dates to plan your testing and upgrade cycles. If Amazon extends support for an RDS for MariaDB version for longer than originally stated, we plan to update this table to reflect the later date.

Note

Dates with only a month and a year are approximate and are updated with an exact date when it's known.

MariaDB major version	Community release date	RDS release date	Community end of life date	RDS end of standard support date
MariaDB 10.6 Current minor version: 10.6.11	6 July 2021	3 February 2022	6 July 2026	July 2026
MariaDB 10.5 Current minor version: 10.5.18	24 June 2020	21 January 2021	24 June 2025	June 2025
MariaDB 10.4 Current minor version: 10.4.27	18 June 2019	6 April 2020	18 June 2024	June 2024
MariaDB 10.3 Current minor version: 10.3.37	25 May 2018	23 October 2018	25 May 2023	23 October 2023

MariaDB major version	Community release date	RDS release date	Community end of life date	RDS end of standard support date
MariaDB 10.2	23 May 2017	5 Jan 2018	23 May 2022	15 Oct 2022
Current minor version: 10.2.44				

MariaDB 10.3 end of life

On October 23, 2023, Amazon RDS is starting the end-of-life process for MariaDB version 10.3 using the following schedule, which includes upgrade recommendations. The end-of-life process ends standard support for this version. We recommend that you upgrade all MariaDB 10.3 DB instances to MariaDB 10.6 as soon as possible. For more information, see [Upgrading the MariaDB DB engine \(p. 998\)](#).

Action or recommendation	Dates
We recommend that you manually upgrade MariaDB 10.3 DB instances to the version of your choice. You can upgrade directly to MariaDB version 10.6.	Now–October 23, 2023
We recommend that you manually upgrade MariaDB 10.3 snapshots to the version of your choice.	Now–October 23, 2023
You can no longer create new MariaDB 10.3 DB instances.	August 23, 2023
You can still create read replicas of existing MariaDB 10.3 DB instances and change them from Single-AZ deployments to Multi-AZ deployments.	
Amazon RDS starts automatic upgrades of your MariaDB 10.3 DB instances to version 10.6.	October 23, 2023
Amazon RDS starts automatic upgrades to version 10.6 for any MariaDB 10.3 DB instances restored from snapshots.	October 23, 2023
Amazon RDS automatically upgrades any remaining MariaDB 10.3 DB instances to version 10.6 whether or not they are in a scheduled maintenance window.	January 23, 2024

MariaDB 10.2 end of life

On October 15, 2022, Amazon RDS is starting the end-of-life process for MariaDB version 10.2 using the following schedule, which includes upgrade recommendations. The end-of-life process ends standard support for this version. We recommend that you upgrade all MariaDB 10.2 DB instances to MariaDB 10.3 or higher as soon as possible. For more information, see [Upgrading the MariaDB DB engine \(p. 998\)](#).

Action or recommendation	Dates
We recommend that you upgrade MariaDB 10.2 DB instances manually to the version of your choice. You can upgrade directly to MariaDB version 10.3 or 10.6.	Now–October 15, 2022
We recommend that you upgrade MariaDB 10.2 snapshots manually to the version of your choice.	Now–October 15, 2022
You can no longer create new MariaDB 10.2 DB instances. You can still create read replicas of existing MariaDB 10.2 DB instances and change them from Single-AZ deployments to Multi-AZ deployments.	July 15, 2022
Amazon RDS starts automatic upgrades of your MariaDB 10.2 DB instances to version 10.3.	October 15, 2022
Amazon RDS starts automatic upgrades to version 10.3 for any MariaDB 10.2 DB instances restored from snapshots.	October 15, 2022
Amazon RDS automatically upgrades any remaining MariaDB 10.2 DB instances to version 10.3 whether or not they are in a scheduled maintenance window.	January 15, 2023

For more information about Amazon RDS for MariaDB 10.2 end of life, see [Announcement: Amazon Relational Database Service \(Amazon RDS\) for MariaDB 10.2 End-of-Life date is October 15, 2022](#).

Deprecated versions for Amazon RDS for MariaDB

Amazon RDS for MariaDB version 10.0, 10.1, and 10.2 are deprecated.

For information about the Amazon RDS deprecation policy for MariaDB, see [Amazon RDS FAQs](#).

Connecting to a DB instance running the MariaDB database engine

After Amazon RDS provisions your DB instance, you can use any standard MariaDB client application or utility to connect to the instance. In the connection string, you specify the Domain Name System (DNS) address from the DB instance endpoint as the host parameter. You also specify the port number from the DB instance endpoint as the port parameter.

You can connect to an Amazon RDS for MariaDB DB instance by using tools like the MySQL command-line client. For more information on using the MySQL command-line client, see [mysql command-line client](#) in the MariaDB documentation. One GUI-based application that you can use to connect is Heidi. For more information, see the [Download HeidiSQL](#) page. For information about installing MySQL (including the MySQL command-line client), see [Installing and upgrading MySQL](#).

Most Linux distributions include the MariaDB client instead of the Oracle MySQL client. To install the MySQL command-line client on most RPM-based Linux distributions, including Amazon Linux 2, run the following command.

```
yum install mariadb
```

To install the MySQL command-line client on most DEB-based Linux distributions, run the following command.

```
apt-get install mariadb-client
```

To check the version of your MySQL command-line client, run the following command.

```
mysql --version
```

To read the MySQL documentation for your current client version, run the following command.

```
man mysql
```

To connect to a DB instance from outside of a virtual private cloud (VPC) based on Amazon VPC, the DB instance must be publicly accessible. Also, access must be granted using the inbound rules of the DB instance's security group, and other requirements must be met. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

You can use SSL encryption on connections to a MariaDB DB instance. For information, see [Using SSL/TLS with a MariaDB DB instance \(p. 992\)](#).

Topics

- [Finding the connection information for a MariaDB DB instance \(p. 986\)](#)
- [Connecting from the MySQL command-line client \(unencrypted\) \(p. 989\)](#)
- [Troubleshooting connections to your MariaDB DB instance \(p. 990\)](#)

Finding the connection information for a MariaDB DB instance

The connection information for a DB instance includes its endpoint, port, and a valid database user, such as the master user. For example, suppose that an endpoint value is mydb.123456789012.us-

`east-1.rds.amazonaws.com`. In this case, the port value is 3306, and the database user is admin. Given this information, you specify the following values in a connection string:

- For host or host name or DNS name, specify `mydb.123456789012.us-east-1.rds.amazonaws.com`.
- For port, specify 3306.
- For user, specify admin.

To connect to a DB instance, use any client for the MariaDB DB engine. For example, you might use the MySQL command-line client or MySQL Workbench.

To find the connection information for a DB instance, you can use the AWS Management Console, the AWS Command Line Interface (AWS CLI) [describe-db-instances](#) command, or the Amazon RDS API [DescribeDBInstances](#) operation to list its details.

Console

To find the connection information for a DB instance in the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases** to display a list of your DB instances.
3. Choose the name of the MariaDB DB instance to display its details.
4. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the AWS RDS console for a database named 'mydb'. The 'Summary' tab is selected, displaying basic information like DB identifier, Role, and Instance. The 'Connectivity & security' tab is active, showing the endpoint and port details. Two specific fields, 'Endpoint' and 'Port', are highlighted with red circles.

Summary

DB identifier	CPU
mydb	2.33%

Role: Instance

Current activity: 0 Connections

Connectivity & security

Endpoint & port	Network
Endpoint: mydb. [REDACTED].us-east-1.rds.amazonaws.com	Available
Port: 3306	VPC: vpc-6E [REDACTED]
	Subnet: default

5. If you need to find the master user name, choose the **Configuration** tab and view the **Master username** value.

AWS CLI

To find the connection information for a MariaDB DB instance by using the AWS CLI, call the [describe-db-instances](#) command. In the call, query for the DB instance ID, endpoint, port, and master user name.

For Linux, macOS, or Unix:

```
aws rds describe-db-instances \
--filters "Name=engine,Values=mariadb" \
--query "[].{DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername}"
```

For Windows:

```
aws rds describe-db-instances ^
--filters "Name=engine,Values=mariadb" ^
--query "[].{DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername}"
```

Your output should be similar to the following.

```
[  
  [  
    "mydb1",  
    "mydb1.123456789012.us-east-1.rds.amazonaws.com",  
    3306,  
    "admin"  
  ],  
  [  
    "mydb2",  
    "mydb2.123456789012.us-east-1.rds.amazonaws.com",  
    3306,  
    "admin"  
  ]  
]
```

RDS API

To find the connection information for a DB instance by using the Amazon RDS API, call the [DescribeDBInstances](#) operation. In the output, find the values for the endpoint address, endpoint port, and master user name.

Connecting from the MySQL command-line client (unencrypted)

Important

Only use an unencrypted MySQL connection when the client and server are in the same VPC and the network is trusted. For information about using encrypted connections, see [Connecting from the MySQL command-line client with SSL/TLS \(encrypted\) \(p. 993\)](#).

To connect to a DB instance using the MySQL command-line client, enter the following command at a command prompt on a client computer. Doing this connects you to a database on a MariaDB DB instance. Substitute the DNS name (endpoint) for your DB instance for `<endpoint>` and the master user name that you used for `<mymasteruser>`. Provide the master password that you used when prompted for a password.

```
mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

After you enter the password for the user, you see output similar to the following.

```
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 10.5.15-MariaDB-log Source distribution
```

```
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
MariaDB [(none)]>
```

Troubleshooting connections to your MariaDB DB instance

Two common causes of connection failures to a new DB instance are the following:

- The DB instance was created using a security group that doesn't authorize connections from the device or Amazon EC2 instance where the MariaDB application or utility is running. The DB instance must have a VPC security group that authorizes the connections. For more information, see [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#).

You can add or edit an inbound rule in the security group. For **Source**, choose **My IP**. This allows access to the DB instance from the IP address detected in your browser.

- The DB instance was created using the default port of 3306, and your company has firewall rules blocking connections to that port from devices in your company network. To fix this failure, recreate the instance with a different port.

For more information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Securing MariaDB DB instance connections

You can manage the security of your MariaDB DB instances.

Topics

- [MariaDB security on Amazon RDS \(p. 991\)](#)
- [Encrypting client connections to MariaDB DB instances with SSL/TLS \(p. 992\)](#)
- [Using new SSL/TLS certificates for MariaDB DB instances \(p. 994\)](#)

MariaDB security on Amazon RDS

Security for MariaDB DB instances is managed at three levels:

- AWS Identity and Access Management controls who can perform Amazon RDS management actions on DB instances. When you connect to AWS using IAM credentials, your IAM account must have IAM policies that grant the permissions required to perform Amazon RDS management operations. For more information, see [Identity and access management for Amazon RDS \(p. 2016\)](#).
- When you create a DB instance, you use a VPC security group to control which devices and Amazon EC2 instances can open connections to the endpoint and port of the DB instance. These connections can be made using Secure Socket Layer (SSL) and Transport Layer Security (TLS). In addition, firewall rules at your company can control whether devices running at your company can open connections to the DB instance.
- Once a connection has been opened to a MariaDB DB instance, authentication of the login and permissions are applied the same way as in a stand-alone instance of MariaDB. Commands such as CREATE USER, RENAME USER, GRANT, REVOKE, and SET PASSWORD work just as they do in stand-alone databases, as does directly modifying database schema tables.

When you create an Amazon RDS DB instance, the master user has the following default privileges:

- alter
- alter routine
- create
- create routine
- create temporary tables
- create user
- create view
- delete
- drop
- event
- execute
- grant option
- index
- insert
- lock tables
- process
- references
- reload

This privilege is limited on MariaDB DB instances. It doesn't grant access to the FLUSH LOGS or FLUSH TABLES WITH READ LOCK operations.

- replication client
- replication slave
- select
- show databases
- show view
- trigger
- update

For more information about these privileges, see [User account management](#) in the MariaDB documentation.

Note

Although you can delete the master user on a DB instance, we don't recommend doing so. To recreate the master user, use the `ModifyDBInstance` API or the `modify-db-instance` AWS CLI and specify a new master user password with the appropriate parameter. If the master user does not exist in the instance, the master user is created with the specified password.

To provide management services for each DB instance, the `rdsadmin` user is created when the DB instance is created. Attempting to drop, rename, change the password for, or change privileges for the `rdsadmin` account results in an error.

To allow management of the DB instance, the standard `kill` and `kill_query` commands have been restricted. The Amazon RDS commands `mysql.rds_kill`, `mysql.rds_kill_query`, and `mysql.rds_kill_query_id` are provided for use in MariaDB and also MySQL so that you can end user sessions or queries on DB instances.

Encrypting client connections to MariaDB DB instances with SSL/TLS

Secure Sockets Layer (SSL) is an industry-standard protocol for securing network connections between client and server. After SSL version 3.0, the name was changed to Transport Layer Security (TLS). Amazon RDS supports SSL/TLS encryption for MariaDB DB instances. Using SSL/TLS, you can encrypt a connection between your application client and your MariaDB DB instance. SSL/TLS support is available in all AWS Regions.

Topics

- [Using SSL/TLS with a MariaDB DB instance \(p. 992\)](#)
- [Connecting from the MySQL command-line client with SSL/TLS \(encrypted\) \(p. 993\)](#)

Using SSL/TLS with a MariaDB DB instance

Amazon RDS creates an SSL/TLS certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL/TLS certificate includes the DB instance endpoint as the Common Name (CN) for the SSL/TLS certificate to guard against spoofing attacks.

An SSL/TLS certificate created by Amazon RDS is the trusted root entity and should work in most cases but might fail if your application does not accept certificate chains. If your application does not accept certificate chains, you might need to use an intermediate certificate to connect to your AWS Region. For

example, you must use an intermediate certificate to connect to the AWS GovCloud (US) Regions using SSL/TLS.

For information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For more information about using SSL/TLS with MySQL, see [Using new SSL/TLS certificates for MariaDB DB instances \(p. 994\)](#).

Amazon RDS for MariaDB supports Transport Layer Security (TLS) versions 1.0, 1.1, 1.2, and 1.3 for all MariaDB versions.

You can require SSL/TLS connections for specific users accounts. For example, you can use one of the following statements, depending on your MariaDB version, to require SSL/TLS connections on the user account `encrypted_user`.

Use the following statement.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

For more information on SSL/TLS connections with MariaDB, see [Securing Connections for Client and Server](#) in the MariaDB documentation.

Connecting from the MySQL command-line client with SSL/TLS (encrypted)

The `mysql` client program parameters are slightly different if you are using the MySQL 5.7 version, the MySQL 8.0 version, or the MariaDB version.

To find out which version you have, run the `mysql` command with the `--version` option. In the following example, the output shows that the client program is from MariaDB.

```
$ mysql --version
mysql Ver 15.1 Distrib 10.5.15-MariaDB, for osx10.15 (x86_64) using readline 5.1
```

Most Linux distributions, such as Amazon Linux, CentOS, SUSE, and Debian have replaced MySQL with MariaDB, and the `mysql` version in them is from MariaDB.

To connect to your DB instance using SSL/TLS, follow these steps:

To connect to a DB instance with SSL/TLS using the MySQL command-line client

1. Download a root certificate that works for all AWS Regions.

For information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

2. Use a MySQL command-line client to connect to a DB instance with SSL/TLS encryption. For the `-h` parameter, substitute the DNS name (endpoint) for your DB instance. For the `--ssl-ca` parameter, substitute the SSL/TLS certificate file name. For the `-P` parameter, substitute the port for your DB instance. For the `-u` parameter, substitute the user name of a valid database user, such as the master user. Enter the master user password when prompted.

The following example shows how to launch the client using the `--ssl-ca` parameter using the MariaDB client:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl -P 3306 -u myadmin -p
```

To require that the SSL/TLS connection verifies the DB instance endpoint against the endpoint in the SSL/TLS certificate, enter the following command:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl-verify-server-cert -P 3306 -u myadmin -p
```

The following example shows how to launch the client using the `--ssl-ca` parameter using the MySQL 5.7 client or later:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl-mode=REQUIRED -P 3306 -u myadmin -p
```

3. Enter the master user password when prompted.

You should see output similar to the following.

```
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.15-MariaDB-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Using new SSL/TLS certificates for MariaDB DB instances

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your RDS DB instances using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.

This topic can help you to determine whether your applications require certificate verification to connect to your DB instances.

Note

Some applications are configured to connect to MariaDB only if they can successfully verify the certificate on the server. For such applications, you must update your client application trust stores to include the new CA certificates.

You can specify the following SSL modes: disabled, preferred, and required. When you use the preferred SSL mode and the CA certificate doesn't exist or isn't up to date, the connection falls back to not using SSL and still connects successfully.

We recommend avoiding preferred mode. In preferred mode, if the connection encounters an invalid certificate, it stops using encryption and proceeds unencrypted.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB instances. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see [Rotating your SSL/TLS certificate \(p. 2007\)](#). For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For information about using SSL/TLS with MariaDB DB instances, see [Using SSL/TLS with a MariaDB DB instance \(p. 992\)](#).

Topics

- Determining whether a client requires certificate verification in order to connect (p. 995)
- Updating your application trust store (p. 996)
- Example Java code for establishing SSL connections (p. 996)

Determining whether a client requires certificate verification in order to connect

You can check whether JDBC clients and MySQL clients require certificate verification to connect.

JDBC

The following example with MySQL Connector/J 8.0 shows one way to check an application's JDBC connection properties to determine whether successful connections require a valid certificate. For more information on all of the JDBC connection options for MySQL, see [Configuration properties](#) in the MySQL documentation.

When using the MySQL Connector/J 8.0, an SSL connection requires verification against the server CA certificate if your connection properties have `sslMode` set to `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

Note

If you use either the MySQL Java Connector v5.1.38 or later, or the MySQL Java Connector v8.0.9 or later to connect to your databases, even if you haven't explicitly configured your applications to use SSL/TLS when connecting to your databases, these client drivers default to using SSL/TLS. In addition, when using SSL/TLS, they perform partial certificate verification and fail to connect if the database server certificate is expired.

MySQL

The following examples with the MySQL Client show two ways to check a script's MySQL connection to determine whether successful connections require a valid certificate. For more information on all of the connection options with the MySQL Client, see [Client-side configuration for encrypted connections](#) in the MySQL documentation.

When using the MySQL 5.7 or MySQL 8.0 Client, an SSL connection requires verification against the server CA certificate if for the `--ssl-mode` option you specify `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-mode=VERIFY_CA
```

When using the MySQL 5.6 Client, an SSL connection requires verification against the server CA certificate if you specify the `--ssl-verify-server-cert` option, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-verify-server-cert
```

Updating your application trust store

For information about updating the trust store for MySQL applications, see [Using TLS/SSL with MariaDB Connector/J](#) in the MariaDB documentation.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

When you update the trust store, you can retain older certificates in addition to adding the new certificates.

If you are using the MariaDB Connector/J JDBC driver in an application, set the following properties in the application.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

When you start the application, set the following properties.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

Example Java code for establishing SSL connections

The following code example shows how to set up the SSL connection using JDBC.

```
private static final String DB_USER = "admin";

private static final String DB_USER = "user name";
private static final String DB_PASSWORD = "password";
// This key store has only the prod root ca.
private static final String KEY_STORE_FILE_PATH = "file-path-to-keystore";
private static final String KEY_STORE_PASS = "keystore-password";

public static void main(String[] args) throws Exception {
    Class.forName("org.mariadb.jdbc.Driver");

    System.setProperty("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
    System.setProperty("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);

    Properties properties = new Properties();
    properties.put("user", DB_USER);
    properties.put("password", DB_PASSWORD);

    Connection connection = DriverManager.getConnection("jdbc:mysql://ssl-mariadb-
public.cni62e2e7kwh.us-east-1.rds.amazonaws.com:3306?useSSL=true", properties);
```

```
Statement stmt=connection.createStatement();
ResultSet rs=stmt.executeQuery("SELECT 1 from dual");
return;
}
```

Important

After you have determined that your database connections use SSL/TLS and have updated your application trust store, you can update your database to use the rds-ca-2019 certificates. For instructions, see step 3 in [Updating your CA certificate by modifying your DB instance \(p. 2007\)](#).

Upgrading the MariaDB DB engine

When Amazon RDS supports a new version of a database engine, you can upgrade your DB instances to the new version. There are two kinds of upgrades for MariaDB DB instances: major version upgrades and minor version upgrades.

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, you must manually perform major version upgrades of your DB instances. You can initiate a major version upgrade by modifying your DB instance. However, before you perform a major version upgrade, we recommend that you follow the instructions in [Major version upgrades for MariaDB \(p. 999\)](#).

In contrast, *minor version upgrades* include only changes that are backward-compatible with existing applications. You can initiate a minor version upgrade manually by modifying your DB instance. Or you can enable the **Auto minor version upgrade** option when creating or modifying a DB instance. Doing so means that your DB instance is automatically upgraded after Amazon RDS tests and approves the new version. For information about performing an upgrade, see [Upgrading a DB instance engine version \(p. 360\)](#).

If your MariaDB DB instance is using read replicas, you must upgrade all of the read replicas before upgrading the source instance. If your DB instance is in a Multi-AZ deployment, both the writer and standby replicas are upgraded. Your DB instance might not be available until the upgrade is complete.

For more information about MariaDB supported versions and version management, see [MariaDB on Amazon RDS versions \(p. 982\)](#).

Note

Database engine upgrades require downtime. The duration of the downtime varies based on the size of your DB instance.

Topics

- [Overview of upgrading \(p. 998\)](#)
- [Major version upgrades for MariaDB \(p. 999\)](#)
- [Upgrading a MariaDB DB instance \(p. 1000\)](#)
- [Automatic minor version upgrades for MariaDB \(p. 1000\)](#)

Overview of upgrading

When you use the AWS Management Console to upgrade a DB instance, it shows the valid upgrade targets for the DB instance. You can also use the following AWS CLI command to identify the valid upgrade targets for a DB instance:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mariadb \
--engine-version version-number \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mariadb ^
--engine-version version-number ^
```

```
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

For example, to identify the valid upgrade targets for a MariaDB version 10.5.15 DB instance, run the following AWS CLI command:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \  
--engine mariadb \  
--engine-version 10.5.15 \  
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^  
--engine mariadb ^  
--engine-version 10.5.15 ^  
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

Amazon RDS takes two DB snapshots during the upgrade process. The first DB snapshot is of the DB instance before any upgrade changes have been made. If the upgrade doesn't work for your databases, you can restore this snapshot to create a DB instance running the old version. The second DB snapshot is taken when the upgrade completes.

Note

Amazon RDS only takes DB snapshots if you have set the backup retention period for your DB instance to a number greater than 0. To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

After the upgrade is complete, you can't revert to the previous version of the database engine. If you want to return to the previous version, restore the first DB snapshot taken to create a new DB instance.

You control when to upgrade your DB instance to a new version supported by Amazon RDS. This level of control helps you maintain compatibility with specific database versions and test new versions with your application before deploying in production. When you are ready, you can perform version upgrades at the times that best fit your schedule.

If your DB instance is using read replication, you must upgrade all of the Read Replicas before upgrading the source instance.

If your DB instance is in a Multi-AZ deployment, both the primary and standby DB instances are upgraded. The primary and standby DB instances are upgraded at the same time and you will experience an outage until the upgrade is complete. The time for the outage varies based on your database engine, engine version, and the size of your DB instance.

Major version upgrades for MariaDB

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, Amazon RDS doesn't apply major version upgrades automatically. You must manually modify your DB instance. We recommend that you thoroughly test any upgrade before applying it to your production instances.

Amazon RDS supports the following in-place upgrades for major versions of the MariaDB database engine:

- Any MariaDB version to MariaDB 10.6

- MariaDB 10.4 to MariaDB 10.5
- MariaDB 10.3 to MariaDB 10.4
- MariaDB 10.2 to MariaDB 10.3

To perform a major version upgrade to MariaDB version 10.6, you can upgrade directly from any MariaDB version to version 10.6.

To perform a major version upgrade to a MariaDB version lower than 10.6, upgrade to each major version in order. For example, to upgrade from version 10.2 to version 10.5, upgrade in the following order: 10.2 to 10.3, 10.3 to 10.4, and then 10.4 to 10.5.

If you are using a custom parameter group, and you perform a major version upgrade, you must specify either a default parameter group for the new DB engine version or create your own custom parameter group for the new DB engine version. Associating the new parameter group with the DB instance requires a customer-initiated database reboot after the upgrade completes. The instance's parameter group status will show pending-reboot if the instance needs to be rebooted to apply the parameter group changes. An instance's parameter group status can be viewed in the AWS console or by using a "describe" call such as `describe-db-instances`.

Upgrading a MariaDB DB instance

For information about manually or automatically upgrading a MariaDB DB instance, see [Upgrading a DB instance engine version \(p. 360\)](#).

Automatic minor version upgrades for MariaDB

If you specify the following settings when creating or modifying a DB instance, you can have your DB instance automatically upgraded.

- The **Auto minor version upgrade** setting is enabled.
- The **Backup retention period** setting is greater than 0.

In the AWS Management Console, these settings are under **Additional configuration**. The following image shows the **Auto minor version upgrade** setting.

Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)
Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Select window
 No preference

Start day	Start time	Duration
Monday ▾	00 ▾ : 00 ▾ UTC	0.5 ▾ hours

For more information about these settings, see [Settings for DB instances \(p. 328\)](#).

For some RDS for MariaDB major versions in some AWS Regions, one minor version is designated by RDS as the automatic upgrade version. After a minor version has been tested and approved by Amazon RDS, the minor version upgrade occurs automatically during your maintenance window. RDS doesn't automatically set newer released minor versions as the automatic upgrade version. Before RDS designates a newer automatic upgrade version, several criteria are considered, such as the following:

- Known security issues
- Bugs in the MariaDB community version
- Overall fleet stability since the minor version was released

You can use the following AWS CLI command to determine the current automatic minor upgrade target version for a specified MariaDB minor version in a specific AWS Region.

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mariadb \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mariadb ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

For example, the following AWS CLI command determines the automatic minor upgrade target for MariaDB minor version 10.2.39 in the US East (Ohio) AWS Region (us-east-2).

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mariadb \
--engine-version 10.2.39 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mariadb ^
--engine-version 10.2.39 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Your output is similar to the following.

DescribeDBEngineVersions	
AutoUpgrade	EngineVersion
True	10.2.40
False	10.2.41
False	10.2.43
False	10.2.44
False	10.3.28
False	10.3.31
False	10.3.32
False	10.3.34
False	10.3.35
False	10.6.5
False	10.6.7
False	10.6.8

In this example, the AutoUpgrade value is True for MariaDB version 10.2.40. So, the automatic minor upgrade target is MariaDB version 10.2.40, which is highlighted in the output.

A MariaDB DB instance is automatically upgraded during your maintenance window if the following criteria are met:

- The **Auto minor version upgrade** setting is enabled.
- The **Backup retention period** setting is greater than 0.
- The DB instance is running a minor DB engine version that is less than the current automatic upgrade minor version.

For more information, see [Automatically upgrading the minor engine version \(p. 362\)](#).

Importing data into a MariaDB DB instance

You can use several different techniques to import data into an RDS for MariaDB DB instance. The best approach depends on the source of the data, the amount of data, and whether the import is done one time or is ongoing. If you are migrating an application along with the data, also consider the amount of downtime that you are willing to experience.

Find techniques to import data into an RDS for MariaDB DB instance in the following table.

Source	Amount of data	One time or ongoing	Application downtime	Technique	More information
Existing MariaDB DB instance	Any	One time or ongoing	Minimal	Create a read replica for ongoing replication. Promote the read replica for one-time creation of a new DB instance.	Working with read replicas (p. 370)
Existing MariaDB or MySQL database	Small	One time	Some	Copy the data directly to your MySQL DB instance using a command-line utility.	Importing data from a MariaDB or MySQL database to a MariaDB or MySQL DB instance (p. 1004)
Data not stored in an existing database	Medium	One time	Some	Create flat files and import them using the <code>mysqlimport</code> utility.	Importing data from any source to a MariaDB or MySQL DB instance (p. 1019)
Existing MariaDB or MySQL database on premises or on Amazon EC2	Any	Ongoing	Minimal	Configure replication with an existing MariaDB or MySQL database as the replication source. You can configure replication into a MariaDB DB instance using MariaDB global transaction identifiers (GTIDs) when the external instance is MariaDB version 10.0.24 or higher, or using binary log coordinates for MySQL instances or MariaDB instances on earlier versions than 10.0.24. MariaDB GTIDs are implemented differently than MySQL GTIDs, which aren't supported by Amazon RDS.	Configuring binary log file position replication with an external source instance (p. 1036) Importing data to an Amazon

Source	Amount of data	One time or ongoing	Application downtime	Technique	More information
					RDS MariaDB or MySQL DB instance with reduced downtime (p. 1006)
Any existing database	Any	One time or ongoing	Minimal	Use AWS Database Migration Service to migrate the database with minimal downtime and, for many database DB engines, continue ongoing replication.	What is AWS Database Migration Service and Using a MySQL-compatible database as a target for AWS DMS in the AWS Database Migration Service User Guide

Note

The mysql system database contains authentication and authorization information required to log into your DB instance and access your data. Dropping, altering, renaming, or truncating tables, data, or other contents of the mysql database in your DB instance can result in errors and might render the DB instance and your data inaccessible. If this occurs, the DB instance can be restored from a snapshot using the AWS CLI [restore-db-instance-from-db-snapshot](#) or recovered using [restore-db-instance-to-point-in-time](#) commands.

Importing data from a MariaDB or MySQL database to a MariaDB or MySQL DB instance

You can also import data from an existing MariaDB or MySQL database to a MySQL or MariaDB DB instance. You do so by copying the database with [mysqldump](#) and piping it directly into the MariaDB or MySQL DB instance. The mysqldump command line utility is commonly used to make backups and transfer data from one MariaDB or MySQL server to another. It's included with MySQL and MariaDB client software.

Note

If you are using a MySQL DB instance and your scenario supports it, it's easier to move data in and out of Amazon RDS by using backup files and Amazon S3. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

A typical mysqldump command to move data from an external database to an Amazon RDS DB instance looks similar to the following.

```
mysqldump -u local_user \
--databases database_name \
--single-transaction \
--compress \
--order-by-primary \
-plocal_password | mysql -u RDS_user \
--port=port_number \
--host=host_name \
-pRDS_password
```

Important

Make sure not to leave a space between the `-p` option and the entered password.

Make sure that you're aware of the following recommendations and considerations:

- Exclude the following schemas from the dump file: `sys`, `performance_schema`, and `information_schema`. The `mysqldump` utility excludes these schemas by default.
- If you need to migrate users and privileges, consider using a tool that generates the data control language (DCL) for recreating them, such as the [pt-show-grants](#) utility.
- To perform the import, make sure the user doing so has access to the DB instance. For more information, see [Controlling access with security groups \(p. 2085\)](#).

The parameters used are as follows:

- `-u local_user` – Use to specify a user name. In the first usage of this parameter, you specify the name of a user account on the local MariaDB or MySQL database identified by the `--databases` parameter.
- `--databases database_name` – Use to specify the name of the database on the local MariaDB or MySQL instance that you want to import into Amazon RDS.
- `--single-transaction` – Use to ensure that all of the data loaded from the local database is consistent with a single point in time. If there are other processes changing the data while `mysqldump` is reading it, using this parameter helps maintain data integrity.
- `--compress` – Use to reduce network bandwidth consumption by compressing the data from the local database before sending it to Amazon RDS.
- `--order-by-primary` – Use to reduce load time by sorting each table's data by its primary key.
- `-plocal_password` – Use to specify a password. In the first usage of this parameter, you specify the password for the user account identified by the first `-u` parameter.
- `-u RDS_user` – Use to specify a user name. In the second usage of this parameter, you specify the name of a user account on the default database for the MariaDB or MySQL DB instance identified by the `--host` parameter.
- `--port port_number` – Use to specify the port for your MariaDB or MySQL DB instance. By default, this is 3306 unless you changed the value when creating the instance.
- `--host host_name` – Use to specify the Domain Name System (DNS) name from the Amazon RDS DB instance endpoint, for example, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. You can find the endpoint value in the instance details in the Amazon RDS Management Console.
- `-pRDS_password` – Use to specify a password. In the second usage of this parameter, you specify the password for the user account identified by the second `-u` parameter.

Make sure to create any stored procedures, triggers, functions, or events manually in your Amazon RDS database. If you have any of these objects in the database that you are copying, then exclude them when

you run `mysqldump`. To do so, include the following parameters with your `mysqldump` command: `--routines=0 --triggers=0 --events=0`.

The following example copies the `world` sample database on the local host to a MySQL DB instance.

For Linux, macOS, or Unix:

```
sudo mysqldump -u localuser \
    --databases world \
    --single-transaction \
    --compress \
    --order-by-primary \
    --routines=0 \
    --triggers=0 \
    --events=0 \
    -plocalpassword | mysql -u rdsuser \
    --port=3306 \
    --host=myinstance.123456789012.us-east-1.rds.amazonaws.com \
    -prdspassword
```

For Windows, run the following command in a command prompt that has been opened by right-clicking **Command Prompt** on the Windows programs menu and choosing **Run as administrator**:

```
mysqldump -u localuser ^
    --databases world ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    --routines=0 ^
    --triggers=0 ^
    --events=0 ^
    -plocalpassword | mysql -u rdsuser ^
    --port=3306 ^
    --host=myinstance.123456789012.us-east-1.rds.amazonaws.com ^
    -prdspassword
```

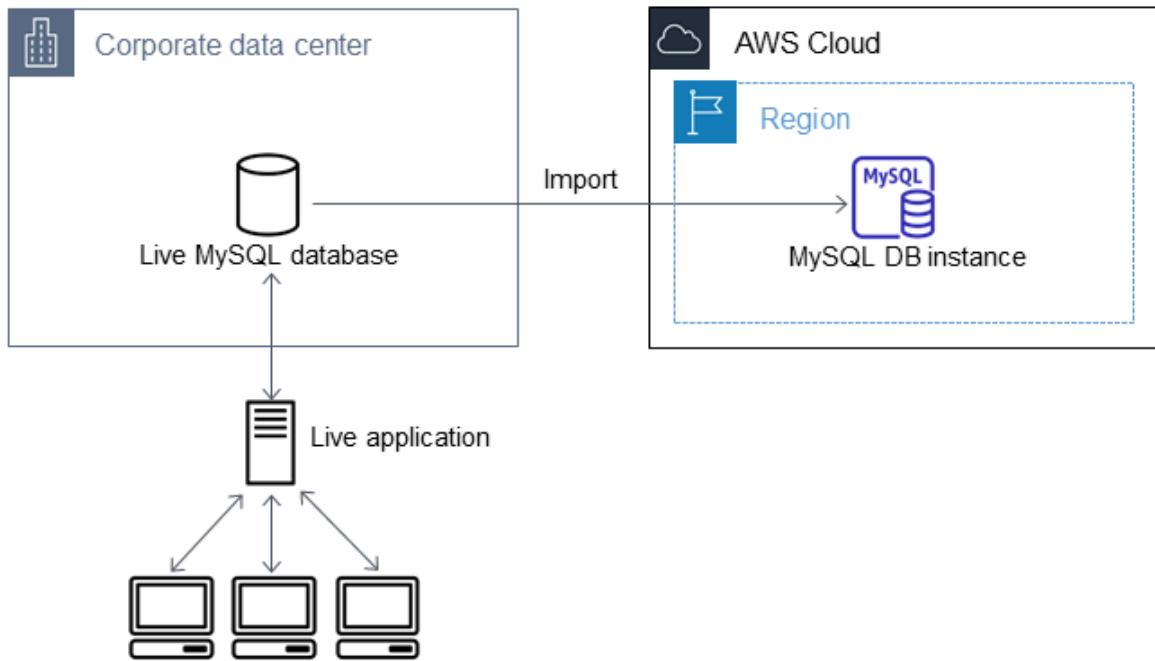
Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime

In some cases, you might need to import data from an external MariaDB or MySQL database that supports a live application to a MariaDB or MySQL DB instance. In these cases, you can use the following procedure to minimize the impact on application availability. This procedure can also help if you are working with a very large database. Here, the procedure helps because you can reduce the cost of the import by reducing the amount of data that is passed across the network to AWS.

In this procedure, you transfer a copy of your database data to an Amazon EC2 instance and import the data into a new Amazon RDS DB instance. You then use replication to bring the Amazon RDS DB instance up-to-date with your live external instance, before redirecting your application to the Amazon RDS DB instance. You configure MariaDB replication based on global transaction identifiers (GTIDs) if the external instance is MariaDB 10.0.24 or higher and the target instance is RDS for MariaDB. Otherwise, you configure replication based on binary log coordinates. We recommend GTID-based replication if your external database supports it due to its enhanced crash-safety features. For more information, see [Global transaction ID](#) in the MariaDB documentation.

Note

If you want to import data into a MySQL DB instance and your scenario supports it, it is easier to move data in and out of Amazon RDS by using backup files and Amazon S3. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

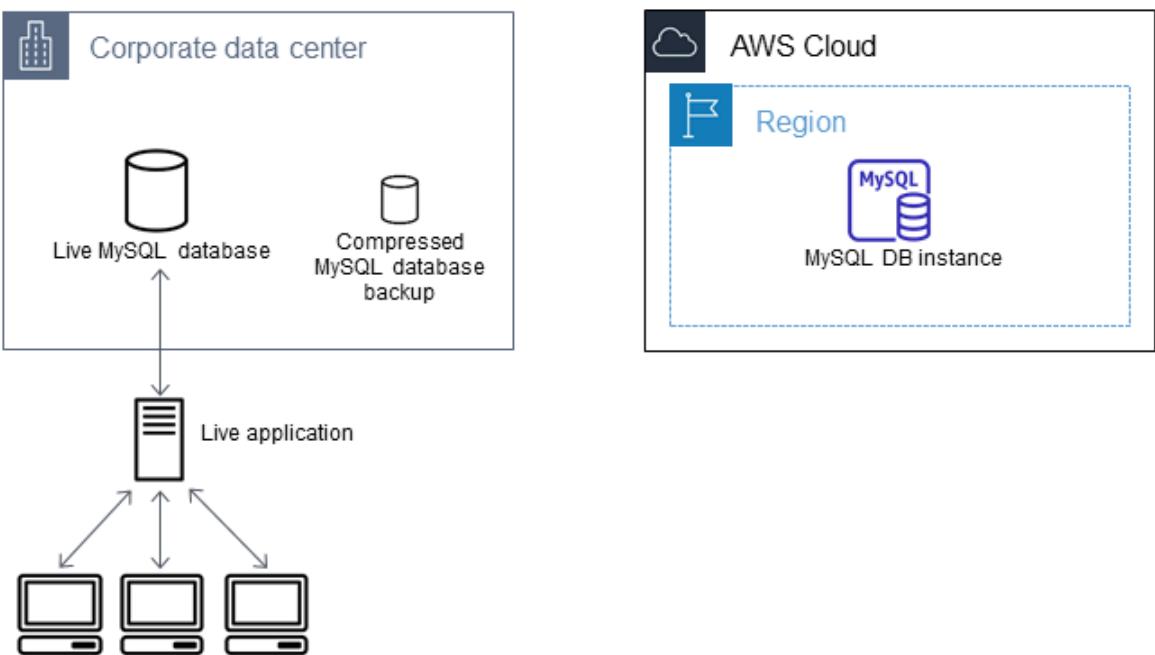


Note

We don't recommend that you use this procedure with source MySQL databases from MySQL versions earlier than version 5.5, due to potential replication issues. For more information, see [Replication compatibility between MySQL versions](#) in the MySQL documentation.

Create a copy of your existing database

The first step in the process of migrating a large amount of data to an Amazon RDS MariaDB or MySQL DB instance with minimal downtime is to create a copy of the source data.



You can use the mysqldump utility to create a database backup in either SQL or delimited-text format. We recommend that you do a test run with each format in a nonproduction environment to see which method minimizes the amount of time that mysqldump runs.

We also recommend that you weigh mysqldump performance against the benefit offered by using the delimited-text format for loading. A backup using delimited-text format creates a tab-separated text file for each table being dumped. To reduce the amount of time required to import your database, you can load these files in parallel using the `LOAD DATA LOCAL INFILE` command. For more information about choosing a mysqldump format and then loading the data, see [Using mysqldump for backups](#) in the MySQL documentation.

Before you start the backup operation, make sure to set the replication options on the MariaDB or MySQL database that you are copying to Amazon RDS. The replication options include turning on binary logging and setting a unique server ID. Setting these options causes your server to start logging database transactions and prepares it to be a source replication instance later in this process.

Note

Use the `--single-transaction` option with mysqldump because it dumps a consistent state of the database. To ensure a valid dump file, don't run data definition language (DDL) statements while mysqldump is running. You can schedule a maintenance window for these operations.

Exclude the following schemas from the dump file: `sys`, `performance_schema`, and `information_schema`. The mysqldump utility excludes these schemas by default.

To migrate users and privileges, consider using a tool that generates the data control language (DCL) for recreating them, such as the [pt-show-grants](#) utility.

To set replication options

1. Edit the `my.cnf` file (this file is usually under `/etc`).

```
sudo vi /etc/my.cnf
```

Add the `log_bin` and `server_id` options to the `[mysqld]` section. The `log_bin` option provides a file name identifier for binary log files. The `server_id` option provides a unique identifier for the server in source-replica relationships.

The following example shows the updated `[mysqld]` section of a `my.cnf` file.

```
[mysqld]
log-bin=mysql-bin
server-id=1
```

For more information, see [the MySQL documentation](#).

2. Restart the `mysql` service.

```
sudo service mysqld restart
```

To create a backup copy of your existing database

1. Create a backup of your data using the mysqldump utility, specifying either SQL or delimited-text format.

Specify `--master-data=2` to create a backup file that can be used to start replication between servers. For more information, see the [mysqldump](#) documentation.

To improve performance and ensure data integrity, use the `--order-by-primary` and `--single-transaction` options of mysqldump.

To avoid including the MySQL system database in the backup, do not use the `--all-databases` option with mysqldump. For more information, see [Creating a data snapshot using mysqldump](#) in the MySQL documentation.

Use `chmod` if necessary to make sure that the directory where the backup file is being created is writeable.

Important

On Windows, run the command window as an administrator.

- To produce SQL output, use the following command.

For Linux, macOS, or Unix:

```
sudo mysqldump \  
  --databases database_name \  
  --master-data=2 \  
  --single-transaction \  
  --order-by-primary \  
  -r backup.sql \  
  -u local_user \  
  -p password
```

For Windows:

```
mysqldump ^  
  --databases database_name ^  
  --master-data=2 ^  
  --single-transaction ^  
  --order-by-primary ^  
  -r backup.sql ^  
  -u local_user ^  
  -p password
```

- To produce delimited-text output, use the following command.

For Linux, macOS, or Unix:

```
sudo mysqldump \  
  --tab=target_directory \  
  --fields-terminated-by ',' ' \  
  --fields-enclosed-by '"' ' \  
  --lines-terminated-by 0x0d0a \  
  database_name \  
  --master-data=2 \  
  --single-transaction \  
  --order-by-primary \  
  -p password
```

For Windows:

```
mysqldump ^  
  --tab=target_directory ^  
  --fields-terminated-by "," ^  
  --fields-enclosed-by "" " ^  
  --lines-terminated-by 0x0d0a ^  
  database_name ^
```

```
--master-data=2 ^  
--single-transaction ^  
--order-by-primary ^  
-p password
```

Note

Make sure to create any stored procedures, triggers, functions, or events manually in your Amazon RDS database. If you have any of these objects in the database that you are copying, exclude them when you run mysqldump. To do so, include the following arguments with your mysqldump command: `--routines=0 --triggers=0 --events=0`.

When using the delimited-text format, a CHANGE MASTER TO comment is returned when you run mysqldump. This comment contains the master log file name and position. If the external instance is other than MariaDB version 10.0.24 or higher, note the values for `MASTER_LOG_FILE` and `MASTER_LOG_POS`. You need these values when setting up replication.

```
-- Position to start replication or point-in-time recovery from  
--  
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

If you are using SQL format, you can get the master log file name and position in the CHANGE MASTER TO comment in the backup file. If the external instance is MariaDB version 10.0.24 or higher, you can get the GTID in the next step.

2. If the external instance you are using is MariaDB version 10.0.24 or higher, you use GTID-based replication. Run `SHOW MASTER STATUS` on the external MariaDB instance to get the binary log file name and position, then convert them to a GTID by running `BINLOG_GTID_POS` on the external MariaDB instance.

```
SELECT BINLOG_GTID_POS('binary log file name', binary log file position);
```

Note the GTID returned; you need it to configure replication.

3. Compress the copied data to reduce the amount of network resources needed to copy your data to the Amazon RDS DB instance. Take note of the size of the backup file; you need this information when determining how large an Amazon EC2 instance to create. When you are done, compress the backup file using GZIP or your preferred compression utility.

- To compress SQL output, use the following command.

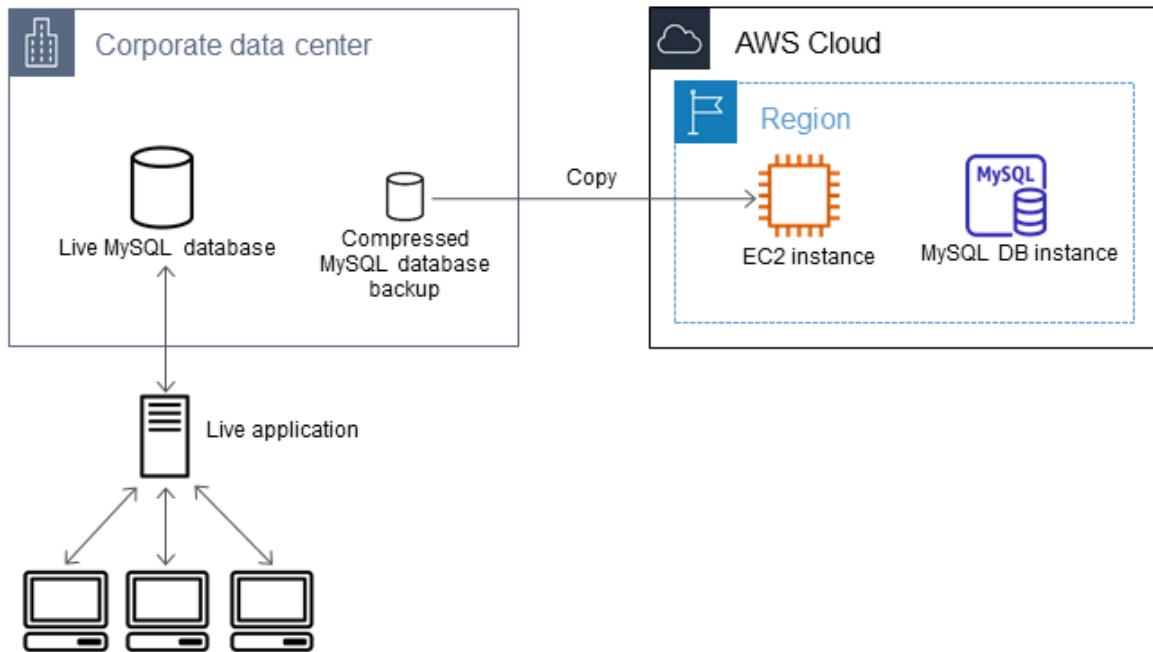
```
gzip backup.sql
```

- To compress delimited-text output, use the following command.

```
tar -zcvf backup.tar.gz target_directory
```

Create an Amazon EC2 instance and copy the compressed database

Copying your compressed database backup file to an Amazon EC2 instance takes fewer network resources than doing a direct copy of uncompressed data between database instances. After your data is in Amazon EC2, you can copy it from there directly to your MariaDB or MySQL DB instance. For you to save on the cost of network resources, your Amazon EC2 instance must be in the same AWS Region as your Amazon RDS DB instance. Having the Amazon EC2 instance in the same AWS Region as your Amazon RDS DB instance also reduces network latency during the import.



To create an Amazon EC2 instance and copy your data

1. In the AWS Region where you plan to create the RDS DB instance to run your MySQL database engine, create a virtual private cloud (VPC), a VPC security group, and a VPC subnet. Ensure that the inbound rules for your VPC security group allow the IP addresses required for your application to connect to AWS. This can be a range of IP addresses (for example, 203 . 0 . 113 . 0/24), or another VPC security group. You can use the [Amazon VPC Management Console](#) to create and manage VPCs, subnets, and security groups. For more information, see [Getting started with Amazon VPC](#) in the *Amazon Virtual Private Cloud Getting Started Guide*.
2. Open the [Amazon EC2 Management Console](#) and choose the AWS Region to contain both your Amazon EC2 instance and your Amazon RDS DB instance. Launch an Amazon EC2 instance using the VPC, subnet, and security group that you created in Step 1. Ensure that you select an instance type with enough storage for your database backup file when it is uncompressed. For details on Amazon EC2 instances, see [Getting started with Amazon EC2 Linux instances](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.
3. To connect to your Amazon RDS DB instance from your Amazon EC2 instance, edit your VPC security group. Add an inbound rule specifying the private IP address of your EC2 instance. You can find the private IP address on the **Details** tab of the **Instance** pane in the EC2 console window. To edit the VPC security group and add an inbound rule, choose **Security Groups** in the EC2 console navigation pane, choose your security group, and then add an inbound rule for MySQL or Aurora specifying the private IP address of your EC2 instance. To learn how to add an inbound rule to a VPC security group, see [Adding and removing rules](#) in the *Amazon VPC User Guide*.
4. Copy your compressed database backup file from your local system to your Amazon EC2 instance. Use chmod if necessary to make sure that you have write permission for the target directory of the Amazon EC2 instance. You can use scp or a Secure Shell (SSH) client to copy the file. The following is an example.

```
$ scp -r -i key_pair.pem backup.sql.gz ec2-user@EC2 DNS:/target_directory/backup.sql.gz
```

Important

Be sure to copy sensitive data using a secure network transfer protocol.

5. Connect to your Amazon EC2 instance and install the latest updates and the MySQL client tools using the following commands.

```
sudo yum update -y  
sudo yum install mysql -y
```

For more information, see [Connect to your instance](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.

Important

This example installs the MySQL client on an Amazon Machine Image (AMI) for an Amazon Linux distribution. To install the MySQL client on a different distribution, such as Ubuntu or RedHat Enterprise Linux, this example doesn't work. For information about installing MySQL, see [Installing and Upgrading MySQL](#) in the MySQL documentation.

6. While connected to your Amazon EC2 instance, decompress your database backup file. The following are examples.

- To decompress SQL output, use the following command.

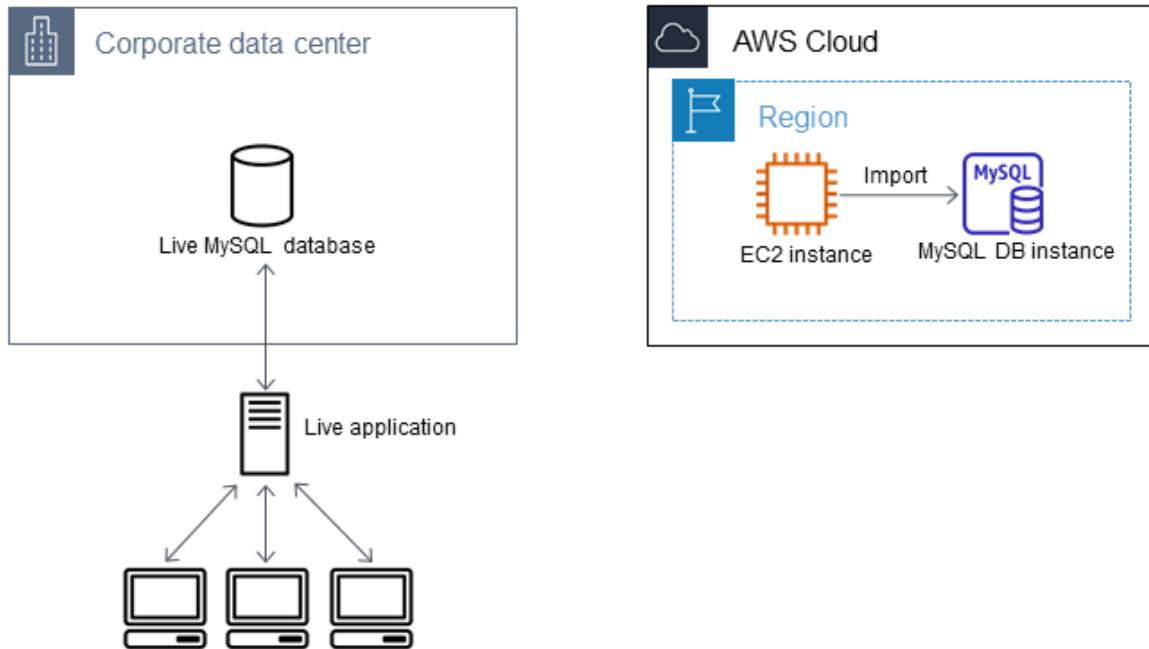
```
gzip backup.sql.gz -d
```

- To decompress delimited-text output, use the following command.

```
tar xzvf backup.tar.gz
```

Create a MySQL or MariaDB DB instance and import data from your Amazon EC2 instance

By creating a MariaDB or MySQL DB instance in the same AWS Region as your Amazon EC2 instance, you can import the database backup file from EC2 faster than over the internet.



To create a MariaDB or MySQL DB instance and import your data

1. Determine which DB instance class and what amount of storage space is required to support the expected workload for this Amazon RDS DB instance. As part of this process, decide what is sufficient space and processing capacity for your data load procedures. Also decide what is required to handle the production workload. You can estimate this based on the size and resources of the source MariaDB or MySQL database. For more information, see [DB instance classes \(p. 10\)](#).
2. Determine if Amazon RDS provisioned I/O operations per second (IOPS) is required to support the workloads. Provisioned IOPS storage delivers fast throughput for online transaction processing (OLTP) workloads, which are I/O intensive. For more information, see [Provisioned IOPS SSD storage \(p. 66\)](#).
3. Open the [Amazon RDS console](#). In the upper-right corner, choose the AWS Region that contains your Amazon EC2 instance.
4. In the navigation pane, choose **Databases**.
5. Choose **Create database**, and then go through the steps to choose options for your DB instance:
 - a. Make sure that **Standard Create** is chosen.
 - b. In the **Engine options** section, choose **MySQL** or **MariaDB**, as appropriate.
 - c. For **Version**, choose the version that is compatible with your source MySQL instance, as follows:
 - If your source instance is MySQL 5.5.x, the Amazon RDS DB instance must be MySQL.
 - If your source instance is MySQL 5.6.x or 5.7.x, the Amazon RDS DB instance must be MySQL or MariaDB.
 - If your source instance is MySQL 8.0.x, the Amazon RDS DB instance must be MySQL 8.0.x.
 - If your source instance is MariaDB 5.5 or higher, the Amazon RDS DB instance must be MariaDB.
 - d. In the **Templates** section, choose **Dev/Test** to skip configuring Multi-AZ deployment and provisioned IOPS storage.
 - e. In the **Settings** section, specify the requested **DB instance identifier** and user information.
 - f. In the **DB instance class** and **Storage** sections, specify the DB instance class and allocated storage size that you want.
 - g. In the **Availability & durability** section, choose **Do not create a standby instance for Multi-AZ deployment**.
 - h. In the **Connectivity** section, choose the same virtual private cloud (VPC) and VPC security group as for your Amazon EC2 instance. This approach ensures that your Amazon EC2 instance and your Amazon RDS instance are visible to each other over the network. Set **Publicly accessible** to **Yes**. To set up replication with your source database as described later, your DB instance must be publicly accessible.

Use the default values for the other settings in this section.

In the **Backup** section, set the backup retention period to **0 days**.

Use the default values for the other settings in this section.

- i. Open the **Additional configuration** section, and specify an **Initial database name**.

Set the **Backup retention period** to **0 days**

Use the default values for the other settings in this section.

- j. Choose **Create database**.

Your new DB instance appears in the **Databases** list with the status **Creating**. Wait for the **Status** of your new DB instance to show as **Available**.

Don't configure multiple Availability Zones, backup retention, or read replicas until after you have imported the database backup. When that import is done, you can set Multi-AZ and backup retention the way that you want them for the production instance. For a detailed walkthrough of creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

6. Review the default configuration options for the Amazon RDS DB instance. In the RDS console navigation pane, choose **Parameter groups**, and then choose the magnifying glass icon next to the **default.mysqlx.x** or **default.mariadb.x** parameter group. If this parameter group doesn't have the configuration options that you want, find a different one that does or create a new parameter group. For more information on creating a parameter group, see [Working with parameter groups \(p. 289\)](#).

To use a different parameter group than the default, associate it with your Amazon RDS DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

7. Connect to the new Amazon RDS DB instance as the master user. Create the users required to support the administrators, applications, and services that need to access the instance. The host name for the Amazon RDS DB instance is the **Endpoint** value for this instance without including the port number. An example is `mysampledb.claxc2oy9ak1.us-west-2.rds.amazonaws.com`. You can find the endpoint value in the instance details in the Amazon RDS Management Console.
8. Connect to your Amazon EC2 instance. For more information, see [Connect to your instance](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.
9. Connect to your Amazon RDS DB instance as a remote host from your Amazon EC2 instance using the `mysql` command. The following is an example.

```
mysql -h host_name -P 3306 -u db_master_user -p
```

The host name is the DNS name from the Amazon RDS DB instance endpoint.

10. At the `mysql` prompt, run the `source` command and pass it the name of your database dump file to load the data into the Amazon RDS DB instance:
 - For SQL format, use the following command.

```
mysql> source backup.sql;
```

- For delimited-text format, first create the database, if it isn't the default database you created when setting up the Amazon RDS DB instance.

```
mysql> create database database_name;
$ mysql> use database_name;
```

Then create the tables.

```
mysql> source table1.sql
$ mysql> source table2.sql
etc...
```

Then import the data.

```
mysql> LOAD DATA LOCAL INFILE 'table1.txt' INTO TABLE table1 FIELDS TERMINATED BY ',' 
ENCLOSED BY ''' LINES TERMINATED BY '0x0d0a';
$ mysql> LOAD DATA LOCAL INFILE 'table2.txt' INTO TABLE table2 FIELDS TERMINATED BY ',' 
ENCLOSED BY ''' LINES TERMINATED BY '0x0d0a';
etc...
```

To improve performance, you can perform these operations in parallel from multiple connections so that all of your tables get created and then loaded at the same time.

Note

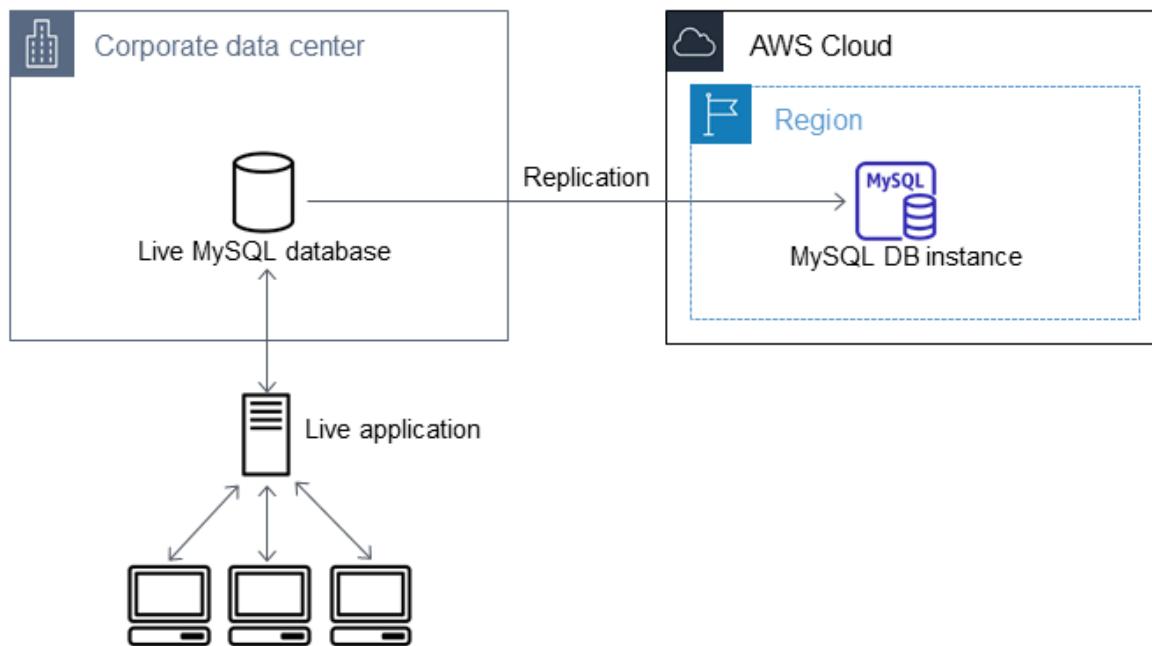
If you used any data-formatting options with `mysqldump` when you initially dumped the table, make sure to use the same options with `mysqlimport` or `LOAD DATA LOCAL INFILE` to ensure proper interpretation of the data file contents.

11. Run a simple `SELECT` query against one or two of the tables in the imported database to verify that the import was successful.

If you no longer need the Amazon EC2 instance used in this procedure, terminate the EC2 instance to reduce your AWS resource usage. To terminate an EC2 instance, see [Terminating an instance](#) in the *Amazon EC2 User Guide*.

Replicate between your external database and new Amazon RDS DB instance

Your source database was likely updated during the time that it took to copy and transfer the data to the MariaDB or MySQL DB instance. That being the case, you can use replication to bring the copied database up-to-date with the source database.



The permissions required to start replication on an Amazon RDS DB instance are restricted and not available to your Amazon RDS master user. Because of this, make sure to use either the Amazon RDS [`mysql.rds_set_external_master` \(p. 1441\)](#) command or the [`mysql.rds_set_external_master_gtid` \(p. 1050\)](#) command to configure replication, and the [`mysql.rds_start_replication` \(p. 1452\)](#) command to start replication between your live database and your Amazon RDS database.

To start replication

Earlier, you turned on binary logging and set a unique server ID for your source database. Now you can set up your Amazon RDS DB instance as a replica with your live database as the source replication instance.

1. In the Amazon RDS Management Console, add the IP address of the server that hosts the source database to the VPC security group for the Amazon RDS DB instance. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.

You might also need to configure your local network to permit connections from the IP address of your Amazon RDS DB instance, so that it can communicate with your source instance. To find the IP address of the Amazon RDS DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the Amazon RDS DB instance endpoint, for example myinstance.123456789012.us-east-1.rds.amazonaws.com. You can find the endpoint value in the instance details in the Amazon RDS Management Console.

2. Using the client of your choice, connect to the source instance and create a user to be used for replication. This account is used solely for replication and must be restricted to your domain to improve security. The following is an example.

MySQL 5.5, 5.6, and 5.7

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

MySQL 8.0

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY 'password';
```

3. For the source instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

MySQL 5.5, 5.6, and 5.7

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'  
IDENTIFIED BY 'password';
```

MySQL 8.0

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

4. If you used SQL format to create your backup file and the external instance is not MariaDB 10.0.24 or higher, look at the contents of that file.

```
cat backup.sql
```

The file includes a CHANGE MASTER TO comment that contains the master log file name and position. This comment is included in the backup file when you use the --master-data option with mysqldump. Note the values for MASTER_LOG_FILE and MASTER_LOG_POS.

```
--  
-- Position to start replication or point-in-time recovery from  
--  
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

If you used delimited text format to create your backup file and the external instance isn't MariaDB 10.0.24 or higher, you should already have binary log coordinates from step 1 of the procedure at "To create a backup copy of your existing database" in this topic.

If the external instance is MariaDB 10.0.24 or higher, you should already have the GTID from which to start replication from step 2 of the procedure at "To create a backup copy of your existing database" in this topic.

5. Make the Amazon RDS DB instance the replica. If the external instance isn't MariaDB 10.0.24 or higher, connect to the Amazon RDS DB instance as the master user and identify the source database as the source replication instance by using the [mysql.rds_set_external_master \(p. 1441\)](#) command. Use the master log file name and master log position that you determined in the previous step if you have a SQL format backup file. Or use the name and position that you determined when creating the backup files if you used delimited-text format. The following is an example.

```
CALL mysql.rds_set_external_master ('myserver.mydomain.com', 3306,  
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);
```

If the external instance is MariaDB 10.0.24 or higher, connect to the Amazon RDS DB instance as the master user and identify the source database as the source replication instance by using the [mysql.rds_set_external_master_gtid \(p. 1050\)](#) command. Use the GTID that you determined in step 2 of the procedure at "To create a backup copy of your existing database" in this topic.. The following is an example.

```
CALL mysql.rds_set_external_master_gtid ('source_server_ip_address', 3306,  
    'ReplicationUser', 'password', 'GTID', 0);
```

The *source_server_ip_address* is the IP address of source replication instance. An EC2 private DNS address is currently not supported.

6. On the Amazon RDS DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

7. On the Amazon RDS DB instance, run the [SHOW REPLICAS STATUS](#) command to determine when the replica is up-to-date with the source replication instance. The results of the SHOW REPLICAS STATUS command include the Seconds_Behind_Master field. When the Seconds_Behind_Master field returns 0, then the replica is up-to-date with the source replication instance.

Note

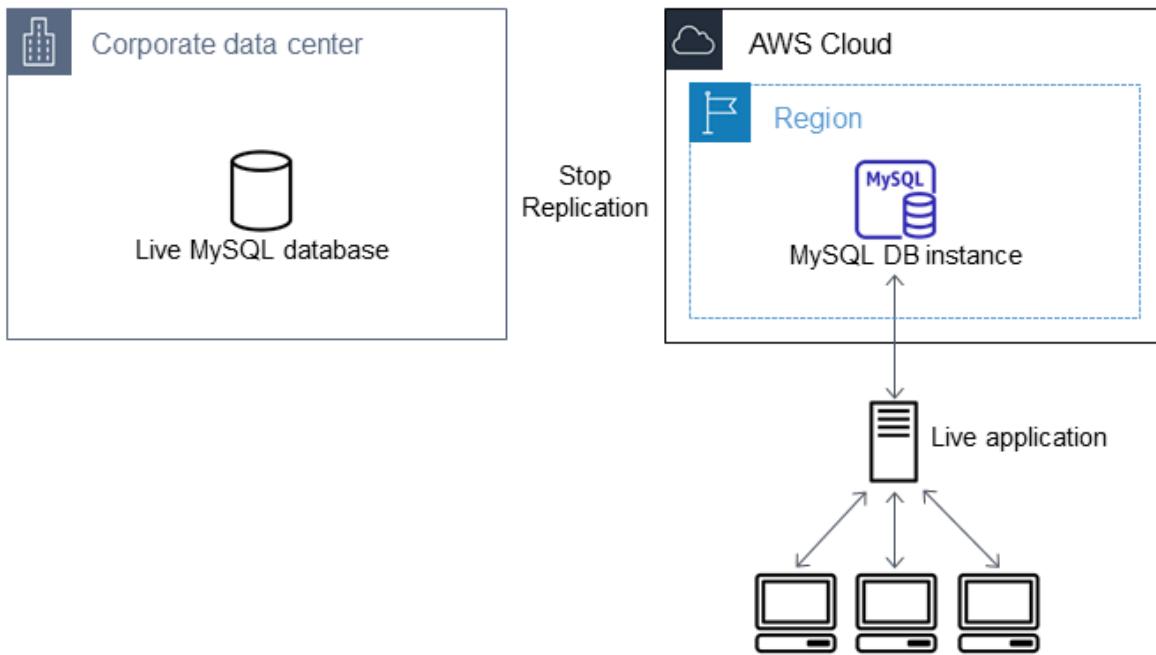
Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICAS STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

For a MariaDB 10.5 or 10.6 DB instance, run the [mysql.rds_replica_status \(p. 1049\)](#) procedure instead of the MySQL command.

8. After the Amazon RDS DB instance is up-to-date, turn on automated backups so you can restore that database if needed. You can turn on or modify automated backups for your Amazon RDS DB instance using the [Amazon RDS Management Console](#). For more information, see [Working with backups \(p. 427\)](#).

Redirect your live application to your Amazon RDS instance

After the MariaDB or MySQL DB instance is up-to-date with the source replication instance, you can now update your live application to use the Amazon RDS instance.



To redirect your live application to your MariaDB or MySQL DB instance and stop replication

1. To add the VPC security group for the Amazon RDS DB instance, add the IP address of the server that hosts the application. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.
2. Verify that the `Seconds_Behind_Master` field in the [SHOW REPLICAS STATUS](#) command results is 0, which indicates that the replica is up-to-date with the source replication instance.

```
SHOW REPLICAS STATUS;
```

Note

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICAS STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

For a MariaDB 10.5 or 10.6 DB instance, run the [mysql.rds_replica_status \(p. 1049\)](#) procedure instead of the MySQL command.

3. Close all connections to the source when their transactions complete.
4. Update your application to use the Amazon RDS DB instance. This update typically involves changing the connection settings to identify the host name and port of the Amazon RDS DB instance, the user account and password to connect with, and the database to use.
5. Stop replication for the Amazon RDS instance using the [mysql.rds_stop_replication \(p. 1454\)](#) command.

```
CALL mysql.rds_stop_replication;
```

6. Run the [mysql.rds_reset_external_master \(p. 1448\)](#) command on your Amazon RDS DB instance to reset the replication configuration so this instance is no longer identified as a replica.

```
CALL mysql.rds_reset_external_master;
```

7. Turn on additional Amazon RDS features such as Multi-AZ support and read replicas. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#) and [Working with read replicas \(p. 370\)](#).

Importing data from any source to a MariaDB or MySQL DB instance

If you have more than 1 GiB of data to load, or if your data is coming from somewhere other than a MariaDB or MySQL database, we recommend creating flat files and loading them with mysqlimport. The mysqlimport utility is another command line utility bundled with the MySQL and MariaDB client software. Its purpose is to load flat files into MySQL or MariaDB. For information about mysqlimport, see [mysqlimport - a data import program](#) in the MySQL documentation.

We also recommend creating DB snapshots of the target Amazon RDS DB instance before and after the data load. Amazon RDS DB snapshots are complete backups of your DB instance that can be used to restore your DB instance to a known state. When you initiate a DB snapshot, I/O operations to your DB instance are momentarily suspended while your database is backed up.

Creating a DB snapshot immediately before the load makes it possible for you to restore the database to its state before the load, if you need to. A DB snapshot taken immediately after the load protects you from having to load the data again in case of a mishap and can also be used to seed new database instances.

The following list shows the steps to take. Each step is discussed in more detail following.

1. Create flat files containing the data to be loaded.
2. Stop any applications accessing the target DB instance.
3. Create a DB snapshot.
4. Consider turning off Amazon RDS automated backups.
5. Load the data using mysqlimport.
6. Enable automated backups again.

Step 1: Create flat files containing the data to be loaded

Use a common format, such as comma-separated values (CSV), to store the data to be loaded. Each table must have its own file; you can't combine data for multiple tables in the same file. Give each file the same name as the table it corresponds to. The file extension can be anything you like. For example, if the table name is sales, the file name might be sales.csv or sales.txt, but not sales_01.csv.

Whenever possible, order the data by the primary key of the table being loaded. Doing this drastically improves load times and minimizes disk storage requirements.

The speed and efficiency of this procedure depends on keeping the size of the files small. If the uncompressed size of any individual file is larger than 1 GiB, split it into multiple files and load each one separately.

On Unix-like systems (including Linux), use the `split` command. For example, the following command splits the sales.csv file into multiple files of less than 1 GiB, splitting only at line breaks (-C 1024m). The new files are named sales.part_00, sales.part_01, and so on.

```
split -C 1024m -d sales.csv sales.part_
```

Similar utilities are available for other operating systems.

Step 2: Stop any applications accessing the target DB instance

Before starting a large load, stop all application activity accessing the target DB instance that you plan to load to. We recommend this particularly if other sessions will be modifying the tables being loaded or tables that they reference. Doing this reduces the risk of constraint violations occurring during the load and improves load performance. It also makes it possible to restore the DB instance to the point just before the load without losing changes made by processes not involved in the load.

Of course, this might not be possible or practical. If you can't stop applications from accessing the DB instance before the load, take steps to ensure the availability and integrity of your data. The specific steps required vary greatly depending upon specific use cases and site requirements.

Step 3: Create a DB snapshot

If you plan to load data into a new DB instance that contains no data, you can skip this step. Otherwise, creating a DB snapshot of your DB instance makes it possible for you to restore the DB instance to the point just before the load, if it becomes necessary. As previously mentioned, when you initiate a DB snapshot, I/O operations to your DB instance are suspended for a few minutes while the database is backed up.

The example following uses the AWS CLI `create-db-snapshot` command to create a DB snapshot of the AcmeRDS instance and give the DB snapshot the identifier "preload".

For Linux, macOS, or Unix:

```
aws rds create-db-snapshot \
--db-instance-identifier AcmeRDS \
--db-snapshot-identifier preload
```

For Windows:

```
aws rds create-db-snapshot ^
--db-instance-identifier AcmeRDS ^
--db-snapshot-identifier preload
```

You can also use the restore from DB snapshot functionality to create test DB instances for dry runs or to undo changes made during the load.

Keep in mind that restoring a database from a DB snapshot creates a new DB instance that, like all DB instances, has a unique identifier and endpoint. To restore the DB instance without changing the endpoint, first delete the DB instance so that you can reuse the endpoint.

For example, to create a DB instance for dry runs or other testing, you give the DB instance its own identifier. In the example, `AcmeRDS-2` is the identifier. The example connects to the DB instance using the endpoint associated with `AcmeRDS-2`.

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-from-db-snapshot \
--db-instance-identifier AcmeRDS-2 \
--db-snapshot-identifier preload
```

For Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
--db-instance-identifier AcmeRDS-2 ^
```

```
--db-snapshot-identifier preload
```

To reuse the existing endpoint, first delete the DB instance and then give the restored database the same identifier.

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \  
  --db-instance-identifier AcmeRDS \  
  --final-db-snapshot-identifier AcmeRDS-Final  
  
aws rds restore-db-instance-from-db-snapshot \  
  --db-instance-identifier AcmeRDS \  
  --db-snapshot-identifier preload
```

For Windows:

```
aws rds delete-db-instance ^  
  --db-instance-identifier AcmeRDS ^  
  --final-db-snapshot-identifier AcmeRDS-Final  
  
aws rds restore-db-instance-from-db-snapshot ^  
  --db-instance-identifier AcmeRDS ^  
  --db-snapshot-identifier preload
```

The preceding example takes a final DB snapshot of the DB instance before deleting it. This is optional but recommended.

Step 4: Consider turning off Amazon RDS automated backups

Warning

Do not turn off automated backups if you need to perform point-in-time recovery.

Turning off automated backups erases all existing backups, so point-in-time recovery isn't possible after automated backups have been turned off. Disabling automated backups is a performance optimization and isn't required for data loads. Manual DB snapshots aren't affected by turning off automated backups. All existing manual DB snapshots are still available for restore.

Turning off automated backups reduces load time by about 25 percent and reduces the amount of storage space required during the load. If you plan to load data into a new DB instance that contains no data, turning off backups is an easy way to speed up the load and avoid using the additional storage needed for backups. However, in some cases you might plan to load into a DB instance that already contains data. If so, weigh the benefits of turning off backups against the impact of losing the ability to perform point-in-time-recovery.

DB instances have automated backups turned on by default (with a one day retention period). To turn off automated backups, set the backup retention period to zero. After the load, you can turn backups back on by setting the backup retention period to a nonzero value. To turn on or turn off backups, Amazon RDS shuts the DB instance down and restarts it to turn MariaDB or MySQL logging on or off.

Use the AWS CLI `modify-db-instance` command to set the backup retention to zero and apply the change immediately. Setting the retention period to zero requires a DB instance restart, so wait until the restart has completed before proceeding.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
  --db-instance-identifier AcmeRDS \  
  --backup-retention 0
```

```
--apply-immediately \
--backup-retention-period 0
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier AcmeRDS ^
--apply-immediately ^
--backup-retention-period 0
```

You can check the status of your DB instance with the AWS CLI `describe-db-instances` command. The following example displays the DB instance status of the AcmeRDS DB instance.

```
aws rds describe-db-instances --db-instance-identifier AcmeRDS --query "[].{DBInstanceState:DBInstanceState}"
```

When the DB instance status is available, you're ready to proceed.

Step 5: Load the data

Use the `mysqlimport` utility to load the flat files into Amazon RDS. The following example tells `mysqlimport` to load all of the files named "sales" with an extension starting with "part_". This is a convenient way to load all of the files created in the "split" example.

Use the `--compress` option to minimize network traffic. The `--fields-terminated-by=','` option is used for CSV files, and the `--local` option specifies that the incoming data is located on the client. Without the `--local` option, the Amazon RDS DB instance looks for the data on the database host, so always specify the `--local` option. For the `--host` option, specify the DB instance endpoint of the RDS for MySQL DB instance.

In the following examples, replace `master_user` with the master username for your DB instance.

Replace `hostname` with the endpoint for your DB instance. An example of a DB instance endpoint is `my-db-instance.123456789012.us-west-2.rds.amazonaws.com`.

For RDS for MySQL version 8.0.15 and higher, run the following statement before using the `mysqlimport` utility.

```
GRANT SESSION_VARIABLES_ADMIN ON *.* TO master_user;
```

For Linux, macOS, or Unix:

```
mysqlimport --local \
--compress \
--user=master_user \
--password \
--host=hostname \
--fields-terminated-by=',' Acme sales.part_*
```

For Windows:

```
mysqlimport --local ^
--compress ^
--user=master_user ^
--password ^
--host=hostname ^
--fields-terminated-by="," Acme sales.part_*
```

For very large data loads, take additional DB snapshots periodically between loading files and note which files have been loaded. If a problem occurs, you can easily resume from the point of the last DB snapshot, avoiding lengthy reloads.

Step 6: Turn Amazon RDS automated backups back on

After the load is finished, turn Amazon RDS automated backups on by setting the backup retention period back to its preload value. As noted earlier, Amazon RDS restarts the DB instance, so be prepared for a brief outage.

The following example uses the AWS CLI `modify-db-instance` command to turn on automated backups for the AcmeRDS DB instance and set the retention period to one day.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier AcmeRDS \
--backup-retention-period 1 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier AcmeRDS ^
--backup-retention-period 1 ^
--apply-immediately
```

Working with MariaDB replication in Amazon RDS

You usually use read replicas to configure replication between Amazon RDS DB instances. For general information about read replicas, see [Working with read replicas \(p. 370\)](#). For specific information about working with read replicas on Amazon RDS for MariaDB, see [Working with MariaDB read replicas \(p. 1024\)](#).

You can also configure replication based on binary log coordinates for a MariaDB DB instance. For MariaDB instances, you can also configure replication based on global transaction IDs (GTIDs), which provides better crash safety. For more information, see [Configuring GTID-based replication with an external source instance \(p. 1034\)](#).

The following are other replication options available with RDS for MariaDB:

- You can set up replication between an RDS for MariaDB DB instance and a MySQL or MariaDB instance that is external to Amazon RDS. For information about configuring replication with an external source, see [Configuring binary log file position replication with an external source instance \(p. 1036\)](#).
- You can configure replication to import databases from a MySQL or MariaDB instance that is external to Amazon RDS, or to export databases to such instances. For more information, see [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1006\)](#) and [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

For any of these replication options, you can use either row-based replication, statement-based, or mixed replication. Row-based replication only replicates the changed rows that result from a SQL statement. Statement-based replication replicates the entire SQL statement. Mixed replication uses statement-based replication when possible, but switches to row-based replication when SQL statements that are unsafe for statement-based replication are run. In most cases, mixed replication is recommended. The binary log format of the DB instance determines whether replication is row-based, statement-based, or mixed. For information about setting the binary log format, see [Binary logging format \(p. 692\)](#).

Topics

- [Working with MariaDB read replicas \(p. 1024\)](#)
- [Configuring GTID-based replication with an external source instance \(p. 1034\)](#)
- [Configuring binary log file position replication with an external source instance \(p. 1036\)](#)

Working with MariaDB read replicas

Following, you can find specific information about working with read replicas on Amazon RDS for MariaDB. For general information about read replicas and instructions for using them, see [Working with read replicas \(p. 370\)](#).

Topics

- [Configuring read replicas with MariaDB \(p. 1025\)](#)
- [Configuring replication filters with MariaDB \(p. 1025\)](#)
- [Configuring delayed replication with MariaDB \(p. 1030\)](#)
- [Updating read replicas with MariaDB \(p. 1031\)](#)
- [Working with Multi-AZ read replica deployments with MariaDB \(p. 1031\)](#)
- [Using cascading read replicas with RDS for MariaDB \(p. 1031\)](#)
- [Monitoring MariaDB read replicas \(p. 1032\)](#)
- [Starting and stopping replication with MariaDB read replicas \(p. 1033\)](#)
- [Troubleshooting a MariaDB read replica problem \(p. 1033\)](#)

Configuring read replicas with MariaDB

Before a MariaDB DB instance can serve as a replication source, make sure to turn on automatic backups on the source DB instance by setting the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica.

You can create up to 15 read replicas from one DB instance within the same Region. For replication to operate effectively, each read replica should have as the same amount of compute and storage resources as the source DB instance. If you scale the source DB instance, also scale the read replicas.

RDS for MariaDB supports cascading read replicas. To learn how to configure cascading read replicas, see [Using cascading read replicas with RDS for MariaDB \(p. 1031\)](#).

You can run multiple read replica create and delete actions at the same time that reference the same source DB instance. When you perform these actions, stay within the limit of 15 read replicas for each source instance.

Configuring replication filters with MariaDB

You can use replication filters to specify which databases and tables are replicated with a read replica. Replication filters can include databases and tables in replication or exclude them from replication.

The following are some use cases for replication filters:

- To reduce the size of a read replica. With replication filtering, you can exclude the databases and tables that aren't needed on the read replica.
- To exclude databases and tables from read replicas for security reasons.
- To replicate different databases and tables for specific use cases at different read replicas. For example, you might use specific read replicas for analytics or sharding.
- For a DB instance that has read replicas in different AWS Regions, to replicate different databases or tables in different AWS Regions.

Note

You can also use replication filters to specify which databases and tables are replicated with a primary MariaDB DB instance that is configured as a replica in an inbound replication topology. For more information about this configuration, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#).

Topics

- [Setting replication filtering parameters for RDS for MariaDB \(p. 1025\)](#)
- [Replication filtering limitations for RDS for MariaDB \(p. 1026\)](#)
- [Replication filtering examples for RDS for MariaDB \(p. 1026\)](#)
- [Viewing the replication filters for a read replica \(p. 1029\)](#)

Setting replication filtering parameters for RDS for MariaDB

To configure replication filters, set the following replication filtering parameters on the read replica:

- `replicate-do-db` – Replicate changes to the specified databases. When you set this parameter for a read replica, only the databases specified in the parameter are replicated.
- `replicate-ignore-db` – Don't replicate changes to the specified databases. When the `replicate-do-db` parameter is set for a read replica, this parameter isn't evaluated.
- `replicate-do-table` – Replicate changes to the specified tables. When you set this parameter for a read replica, only the tables specified in the parameter are replicated. Also, when the `replicate-do-`

`db` or `replicate-ignore-db` parameter is set, the database that includes the specified tables must be included in replication with the read replica.

- `replicate-ignore-table` – Don't replicate changes to the specified tables. When the `replicate-do-table` parameter is set for a read replica, this parameter isn't evaluated.
- `replicate-wild-do-table` – Replicate tables based on the specified database and table name patterns. The `%` and `_` wildcard characters are supported. When the `replicate-do-db` or `replicate-ignore-db` parameter is set, make sure to include the database that includes the specified tables in replication with the read replica.
- `replicate-wild-ignore-table` – Don't replicate tables based on the specified database and table name patterns. The `%` and `_` wildcard characters are supported. When the `replicate-do-table` or `replicate-wild-do-table` parameter is set for a read replica, this parameter isn't evaluated.

The parameters are evaluated in the order that they are listed. For more information about how these parameters work, see [the MariaDB documentation](#).

By default, each of these parameters has an empty value. On each read replica, you can use these parameters to set, change, and delete replication filters. When you set one of these parameters, separate each filter from others with a comma.

You can use the `%` and `_` wildcard characters in the `replicate-wild-do-table` and `replicate-wild-ignore-table` parameters. The `%` wildcard matches any number of characters, and the `_` wildcard matches only one character.

The binary logging format of the source DB instance is important for replication because it determines the record of data changes. The setting of the `binlog_format` parameter determines whether the replication is row-based or statement-based. For more information, see [Binary logging format \(p. 692\)](#).

Note

All data definition language (DDL) statements are replicated as statements, regardless of the `binlog_format` setting on the source DB instance.

Replication filtering limitations for RDS for MariaDB

The following limitations apply to replication filtering for RDS for MariaDB:

- Each replication filtering parameter has a 2,000-character limit.
- Commas aren't supported in replication filters.
- The MariaDB `binlog_do_db` and `binlog_ignore_db` options for binary log filtering aren't supported.
- Replication filtering doesn't support XA transactions.

For more information, see [Restrictions on XA Transactions](#) in the MySQL documentation.

- Replication filtering isn't supported for RDS for MariaDB version 10.2.

Replication filtering examples for RDS for MariaDB

To configure replication filtering for a read replica, modify the replication filtering parameters in the parameter group associated with the read replica.

Note

You can't modify a default parameter group. If the read replica is using a default parameter group, create a new parameter group and associate it with the read replica. For more information on DB parameter groups, see [Working with parameter groups \(p. 289\)](#).

You can set parameters in a parameter group using the AWS Management Console, AWS CLI, or RDS API. For information about setting parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#). When you set parameters in a parameter group, all of the DB instances associated with the parameter

group use the parameter settings. If you set the replication filtering parameters in a parameter group, make sure that the parameter group is associated only with read replicas. Leave the replication filtering parameters empty for source DB instances.

The following examples set the parameters using the AWS CLI. These examples set `ApplyMethod` to `immediate` so that the parameter changes occur immediately after the CLI command completes. If you want a pending change to be applied after the read replica is rebooted, set `ApplyMethod` to `pending-reboot`.

The following examples set replication filters:

- [Including databases in replication](#)
- [Including tables in replication](#)
- [Including tables in replication with wildcard characters](#)
- [Escaping wildcard characters in names](#)
- [Excluding databases from replication](#)
- [Excluding tables from replication](#)
- [Excluding tables from replication using wildcard characters](#)

Example Including databases in replication

The following example includes the `mydb1` and `mydb2` databases in replication. When you set `replicate-do-db` for a read replica, only the databases specified in the parameter are replicated.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
"ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
"ApplyMethod":"immediate"}]"
```

Example Including tables in replication

The following example includes the `table1` and `table2` tables in database `mydb1` in replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-do-table", "ParameterValue":
"mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-do-table", "ParameterValue":
"mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

Example Including tables in replication using wildcard characters

The following example includes tables with names that begin with `orders` and `returns` in database `mydb` in replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

Example Escaping wildcard characters in names

The following example shows you how to use the escape character `\` to escape a wildcard character that is part of a name.

Assume that you have several table names in database `mydb1` that start with `my_table`, and you want to include these tables in replication. The table names include an underscore, which is also a wildcard character, so the example escapes the underscore in the table names.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my\_\_table%", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my\_\_table%", "ApplyMethod":"immediate"}]"
```

Example Excluding databases from replication

The following example excludes the `mydb1` and `mydb2` databases from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue": "mydb1,mydb2", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
```

```
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue": "mydb1,mydb2",
"ApplyMethod":"immediate"}]"
```

Example Excluding tables from replication

The following example excludes tables `table1` and `table2` in database `mydb1` from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue": "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue": "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

Example Excluding tables from replication using wildcard characters

The following example excludes tables with names that begin with `orders` and `returns` in database `mydb` from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

Viewing the replication filters for a read replica

You can view the replication filters for a read replica in the following ways:

- Check the settings of the replication filtering parameters in the parameter group associated with the read replica.

For instructions, see [Viewing parameter values for a DB parameter group \(p. 301\)](#).

- In a MariaDB client, connect to the read replica and run the `SHOW REPLICAS STATUS` statement.

In the output, the following fields show the replication filters for the read replica:

- `Replicate_Do_DB`
- `Replicate_Ignore_DB`
- `Replicate_Do_Table`
- `Replicate_Ignore_Table`

- Replicate_Wild_Do_Table
- Replicate_Wild_Ignore_Table

For more information about these fields, see [Checking Replication Status](#) in the MySQL documentation.

Note

Previous versions of MariaDB used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MariaDB version before 10.5, then use SHOW SLAVE STATUS.

Configuring delayed replication with MariaDB

You can use delayed replication as a strategy for disaster recovery. With delayed replication, you specify the minimum amount of time, in seconds, to delay replication from the source to the read replica. In the event of a disaster, such as a table deleted unintentionally, you complete the following steps to recover from the disaster quickly:

- Stop replication to the read replica before the change that caused the disaster is sent to it.
To stop replication, use the [mysql.rds_stop_replication \(p. 1454\)](#) stored procedure.
- Promote the read replica to be the new source DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Note

- Delayed replication is supported for MariaDB 10.6 and higher.
- Use stored procedures to configure delayed replication. You can't configure delayed replication with the AWS Management Console, the AWS CLI, or the Amazon RDS API.
- You can use replication based on global transaction identifiers (GTIDs) in a delayed replication configuration.

Topics

- [Configuring delayed replication during read replica creation \(p. 1030\)](#)
- [Modifying delayed replication for an existing read replica \(p. 1031\)](#)
- [Promoting a read replica \(p. 1031\)](#)

Configuring delayed replication during read replica creation

To configure delayed replication for any future read replica created from a DB instance, run the [mysql.rds_set_configuration \(p. 1459\)](#) stored procedure with the target_delay parameter.

To configure delayed replication during read replica creation

1. Using a MariaDB client, connect to the MariaDB DB instance to be the source for read replicas as the master user.
2. Run the [mysql.rds_set_configuration \(p. 1459\)](#) stored procedure with the target_delay parameter.

For example, run the following stored procedure to specify that replication is delayed by at least one hour (3,600 seconds) for any read replica created from the current DB instance.

```
call mysql.rds_set_configuration('target delay', 3600);
```

Note

After running this stored procedure, any read replica you create using the AWS CLI or Amazon RDS API is configured with replication delayed by the specified number of seconds.

Modifying delayed replication for an existing read replica

To modify delayed replication for an existing read replica, run the [mysql.rds_set_source_delay \(p. 1451\)](#) stored procedure.

To modify delayed replication for an existing read replica

1. Using a MariaDB client, connect to the read replica as the master user.
2. Use the [mysql.rds_stop_replication \(p. 1454\)](#) stored procedure to stop replication.
3. Run the [mysql.rds_set_source_delay \(p. 1451\)](#) stored procedure.

For example, run the following stored procedure to specify that replication to the read replica is delayed by at least one hour (3600 seconds).

```
call mysql.rds_set_source_delay(3600);
```

4. Use the [mysql.rds_start_replication \(p. 1452\)](#) stored procedure to start replication.

Promoting a read replica

After replication is stopped, in a disaster recovery scenario, you can promote a read replica to be the new source DB instance. For information about promoting a read replica, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Updating read replicas with MariaDB

Read replicas are designed to support read queries, but you might need occasional updates. For example, you might need to add an index to speed the specific types of queries accessing the replica. You can enable updates by setting the `read_only` parameter to `0` in the DB parameter group for the read replica.

Working with Multi-AZ read replica deployments with MariaDB

You can create a read replica from either single-AZ or Multi-AZ DB instance deployments. You use Multi-AZ deployments to improve the durability and availability of critical data, but you can't use the Multi-AZ secondary to serve read-only queries. Instead, you can create read replicas from high-traffic Multi-AZ DB instances to offload read-only queries. If the source instance of a Multi-AZ deployment fails over to the secondary, any associated read replicas automatically switch to use the secondary (now primary) as their replication source. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

Using cascading read replicas with RDS for MariaDB

RDS for MariaDB supports cascading read replicas. With *cascading read replicas*, you can scale reads without adding overhead to your source RDS for MariaDB DB instance.

With cascading read replicas, your RDS for MariaDB DB instance sends data to the first read replica in the chain. That read replica then sends data to the second replica in the chain, and so on. The end result is

that all read replicas in the chain have the changes from the RDS for MariaDB DB instance, but without the overhead solely on the source DB instance.

You can create a series of up to three read replicas in a chain from a source RDS for MariaDB DB instance. For example, suppose that you have an RDS for MariaDB DB instance, `mariadb-main`. You can do the following:

- Starting with `mariadb-main`, create the first read replica in the chain, `read-replica-1`.
- Next, from `read-replica-1`, create the next read replica in the chain, `read-replica-2`.
- Finally, from `read-replica-2`, create the third read replica in the chain, `read-replica-3`.

You can't create another read replica beyond this third cascading read replica in the series for `mariadb-main`. A complete series of instances from an RDS for MariaDB source DB instance through to the end of a series of cascading read replicas can consist of at most four DB instances.

For cascading read replicas to work, each source RDS for MariaDB DB instance must have automated backups turned on. To turn on automatic backups on a read replica, first create the read replica, and then modify the read replica to turn on automatic backups. For more information, see [Creating a read replica \(p. 375\)](#).

As with any read replica, you can promote a read replica that's part of a cascade. Promoting a read replica from within a chain of read replicas removes that replica from the chain. For example, suppose that you want to move some of the workload from your `mariadb-main` DB instance to a new instance for use by the accounting department only. Assuming the chain of three read replicas from the example, you decide to promote `read-replica-2`. The chain is affected as follows:

- Promoting `read-replica-2` removes it from the replication chain.
 - It is now a full read/write DB instance.
 - It continues replicating to `read-replica-3`, just as it was doing before promotion.
- Your `mariadb-main` continues replicating to `read-replica-1`.

For more information about promoting read replicas, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Monitoring MariaDB read replicas

For MariaDB read replicas, you can monitor replication lag in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric. The ReplicaLag metric reports the value of the `Seconds_Behind_Master` field of the `SHOW REPLICA STATUS` command.

Note

Previous versions of MariaDB used `SHOW SLAVE STATUS` instead of `SHOW REPLICA STATUS`. If you are using a MariaDB version before 10.5, then use `SHOW SLAVE STATUS`.

Common causes for replication lag for MariaDB are the following:

- A network outage.
- Writing to tables with indexes on a read replica. If the `read_only` parameter is not set to 0 on the read replica, it can break replication.
- Using a nontransactional storage engine such as MyISAM. Replication is only supported for the InnoDB storage engine on MariaDB.

When the ReplicaLag metric reaches 0, the replica has caught up to the source DB instance. If the ReplicaLag metric returns -1, then replication is currently not active. `ReplicaLag = -1` is equivalent to `Seconds_Behind_Master = NULL`.

Starting and stopping replication with MariaDB read replicas

You can stop and restart the replication process on an Amazon RDS DB instance by calling the system stored procedures [mysql.rds_stop_replication \(p. 1454\)](#) and [mysql.rds_start_replication \(p. 1452\)](#). You can do this when replicating between two Amazon RDS instances for long-running operations such as creating large indexes. You also need to stop and start replication when importing or exporting databases. For more information, see [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#) and [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

If replication is stopped for more than 30 consecutive days, either manually or due to a replication error, Amazon RDS ends replication between the source DB instance and all read replicas. It does so to prevent increased storage requirements on the source DB instance and long failover times. The read replica DB instance is still available. However, replication can't be resumed because the binary logs required by the read replica are deleted from the source DB instance after replication is ended. You can create a new read replica for the source DB instance to reestablish replication.

Troubleshooting a MariaDB read replica problem

The replication technologies for MariaDB are asynchronous. Because they are asynchronous, occasional BinLogDiskUsage increases on the source DB instance and ReplicaLag on the read replica are to be expected. For example, a high volume of write operations to the source DB instance can occur in parallel. In contrast, write operations to the read replica are serialized using a single I/O thread, which can lead to a lag between the source instance and read replica. For more information about read-only replicas in the MariaDB documentation, go to [Replication overview](#).

You can do several things to reduce the lag between updates to a source DB instance and the subsequent updates to the read replica, such as the following:

- Sizing a read replica to have a storage size and DB instance class comparable to the source DB instance.
- Ensuring that parameter settings in the DB parameter groups used by the source DB instance and the read replica are compatible. For more information and an example, see the discussion of the `max_allowed_packet` parameter later in this section.

Amazon RDS monitors the replication status of your read replicas and updates the `Replication State` field of the read replica instance to `Error` if replication stops for any reason. An example might be if DML queries run on your read replica conflict with the updates made on the source DB instance.

You can review the details of the associated error thrown by the MariaDB engine by viewing the `Replication Error` field. Events that indicate the status of the read replica are also generated, including [RDS-EVENT-0045 \(p. 675\)](#), [RDS-EVENT-0046 \(p. 675\)](#), and [RDS-EVENT-0047 \(p. 672\)](#). For more information about events and subscribing to events, see [Working with Amazon RDS event notification \(p. 650\)](#). If a MariaDB error message is returned, review the error in the [MariaDB error message documentation](#).

One common issue that can cause replication errors is when the value for the `max_allowed_packet` parameter for a read replica is less than the `max_allowed_packet` parameter for the source DB instance. The `max_allowed_packet` parameter is a custom parameter that you can set in a DB parameter group that is used to specify the maximum size of DML code that can be run on the database. In some cases, the `max_allowed_packet` parameter value in the DB parameter group associated with a source DB instance is smaller than the `max_allowed_packet` parameter value in the DB parameter group associated with the source's read replica. In these cases, the replication process can throw an error (Packet bigger than '`max_allowed_packet`' bytes) and stop replication. You can fix the error by having the source and read replica use DB parameter groups with the same `max_allowed_packet` parameter values.

Other common situations that can cause replication errors include the following:

- Writing to tables on a read replica. If you are creating indexes on a read replica, you need to have the `read_only` parameter set to `0` to create the indexes. If you are writing to tables on the read replica, it might break replication.
- Using a non-transactional storage engine such as MyISAM. read replicas require a transactional storage engine. Replication is only supported for the InnoDB storage engine on MariaDB.
- Using unsafe nondeterministic queries such as `SYSDATE()`. For more information, see [Determination of safe and unsafe statements in binary logging](#).

If you decide that you can safely skip an error, you can follow the steps described in [Skipping the current replication error \(p. 1428\)](#). Otherwise, you can delete the read replica and create an instance using the same DB instance identifier so that the endpoint remains the same as that of your old read replica. If a replication error is fixed, the Replication State changes to *replicating*.

For MariaDB DB instances, in some cases read replicas can't be switched to the secondary if some binary log (binlog) events aren't flushed during the failure. In these cases, manually delete and recreate the read replicas. You can reduce the chance of this happening by setting the following parameter values: `sync_binlog=1` and `innodb_flush_log_at_trx_commit=1`. These settings might reduce performance, so test their impact before implementing the changes in a production environment.

Configuring GTID-based replication with an external source instance

You can set up replication based on global transaction identifiers (GTIDs) from an external MariaDB instance of version 10.0.24 or higher into an RDS for MariaDB DB instance. Follow these guidelines when you set up an external source instance and a replica on Amazon RDS:

- Monitor failover events for the RDS for MariaDB DB instance that is your replica. If a failover occurs, then the DB instance that is your replica might be recreated on a new host with a different network address. For information on how to monitor failover events, see [Working with Amazon RDS event notification \(p. 650\)](#).
- Maintain the binary logs (binlogs) on your source instance until you have verified that they have been applied to the replica. This maintenance ensures that you can restore your source instance in the event of a failure.
- Turn on automated backups on your MariaDB DB instance on Amazon RDS. Turning on automated backups ensures that you can restore your replica to a particular point in time if you need to resynchronize your source instance and replica. For information on backups and Point-In-Time Restore, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

Note

The permissions required to start replication on a MariaDB DB instance are restricted and not available to your Amazon RDS master user. Because of this, you must use the Amazon RDS `mysql.rds_set_external_master_gtid (p. 1050)` and `mysql.rds_start_replication (p. 1452)` commands to set up replication between your live database and your RDS for MariaDB database.

To start replication between an external source instance and a MariaDB DB instance on Amazon RDS, use the following procedure.

To start replication

1. Make the source MariaDB instance read-only:

```
mysql> FLUSH TABLES WITH READ LOCK;
```

```
mysql> SET GLOBAL read_only = ON;
```

2. Get the current GTID of the external MariaDB instance. You can do this by using mysql or the query editor of your choice to run `SELECT @@gtid_current_pos;`.

The GTID is formatted as <domain-id>-<server-id>-<sequence-id>. A typical GTID looks something like **0-1234510749-1728**. For more information about GTIDs and their component parts, see [Global transaction ID](#) in the MariaDB documentation.

3. Copy the database from the external MariaDB instance to the MariaDB DB instance using mysqldump. For very large databases, you might want to use the procedure in [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#).

For Linux, macOS, or Unix:

```
mysqldump \  
  --databases database_name \  
  --single-transaction \  
  --compress \  
  --order-by-primary \  
  -u local_user \  
  -plocal_password | mysql \  
    --host=hostname \  
    --port=3306 \  
    -u RDS_user_name \  
    -pRDS_password
```

For Windows:

```
mysqldump ^  
  --databases database_name ^  
  --single-transaction ^  
  --compress ^  
  --order-by-primary \  
  -u local_user \  
  -plocal_password | mysql ^  
    --host=hostname ^  
    --port=3306 ^  
    -u RDS_user_name ^  
    -pRDS_password
```

Note

Make sure that there isn't a space between the `-p` option and the entered password.

Use the `--host`, `--user` (`-u`), `--port` and `-p` options in the mysql command to specify the host name, user name, port, and password to connect to your MariaDB DB instance. The host name is the DNS name from the MariaDB DB instance endpoint, for example `myinstance.123456789012.us-east-1.rds.amazonaws.com`. You can find the endpoint value in the instance details in the [Amazon RDS Management Console](#).

4. Make the source MariaDB instance writeable again.

```
mysql> SET GLOBAL read_only = OFF;  
mysql> UNLOCK TABLES;
```

5. In the Amazon RDS Management Console, add the IP address of the server that hosts the external MariaDB database to the VPC security group for the MariaDB DB instance. For more information on modifying a VPC security group, go to [Security groups for your VPC](#) in the [Amazon Virtual Private Cloud User Guide](#).

The IP address can change when the following conditions are met:

- You are using a public IP address for communication between the external source instance and the DB instance.
- The external source instance was stopped and restarted.

If these conditions are met, verify the IP address before adding it.

You might also need to configure your local network to permit connections from the IP address of your MariaDB DB instance, so that it can communicate with your external MariaDB instance. To find the IP address of the MariaDB DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the MariaDB DB instance endpoint.

6. Using the client of your choice, connect to the external MariaDB instance and create a MariaDB user to be used for replication. This account is used solely for replication and must be restricted to your domain to improve security. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. For the external MariaDB instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Make the MariaDB DB instance the replica. Connect to the MariaDB DB instance as the master user and identify the external MariaDB database as the replication source instance by using the [mysql.rds_set_external_master_gtid \(p. 1050\)](#) command. Use the GTID that you determined in Step 2. The following is an example.

```
CALL mysql.rds_set_external_master_gtid ('mymasterserver.mydomain.com', 3306,  
'repl_user', 'password', 'GTID', 0);
```

9. On the MariaDB DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

Configuring binary log file position replication with an external source instance

You can set up replication between an RDS for MySQL or MariaDB DB instance and a MySQL or MariaDB instance that is external to Amazon RDS using binary log file replication.

Topics

- [Before you begin \(p. 1037\)](#)
- [Configuring binary log file position replication with an external source instance \(p. 1037\)](#)

Before you begin

You can configure replication using the binary log file position of replicated transactions.

The permissions required to start replication on an Amazon RDS DB instance are restricted and not available to your Amazon RDS master user. Because of this, make sure that you use the Amazon RDS [mysql.rds_set_external_master \(p. 1441\)](#) and [mysql.rds_start_replication \(p. 1452\)](#) commands to set up replication between your live database and your Amazon RDS database.

To set the binary logging format for a MySQL or MariaDB database, update the `binlog_format` parameter. If your DB instance uses the default DB instance parameter group, create a new DB parameter group to modify `binlog_format` settings. We recommend that you use the default setting for `binlog_format`, which is `MIXED`. However, you can also set `binlog_format` to `ROW` or `STATEMENT` if you need a specific binary log (`binlog`) format. Reboot your DB instance for the change to take effect.

For information about setting the `binlog_format` parameter, see [Configuring MySQL binary logging \(p. 706\)](#). For information about the implications of different MySQL replication types, see [Advantages and disadvantages of statement-based and row-based replication](#) in the MySQL documentation.

Configuring binary log file position replication with an external source instance

Follow these guidelines when you set up an external source instance and a replica on Amazon RDS:

- Monitor failover events for the Amazon RDS DB instance that is your replica. If a failover occurs, then the DB instance that is your replica might be recreated on a new host with a different network address. For information on how to monitor failover events, see [Working with Amazon RDS event notification \(p. 650\)](#).
- Maintain the binlogs on your source instance until you have verified that they have been applied to the replica. This maintenance makes sure that you can restore your source instance in the event of a failure.
- Turn on automated backups on your Amazon RDS DB instance. Turning on automated backups makes sure that you can restore your replica to a particular point in time if you need to re-synchronize your source instance and replica. For information on backups and point-in-time restore, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

To configure binary log file replication with an external source instance

1. Make the source MySQL or MariaDB instance read-only.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Run the `SHOW MASTER STATUS` command on the source MySQL or MariaDB instance to determine the binlog location.

You receive output similar to the following example.

File	Position
mysql-bin-changelog.000031	107

3. Copy the database from the external instance to the Amazon RDS DB instance using `mysqldump`. For very large databases, you might want to use the procedure in [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#).

For Linux, macOS, or Unix:

```
mysqldump --databases database_name \
    --single-transaction \
    --compress \
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql \
    --host=hostname \
    --port=3306 \
    -u RDS_user_name \
    -pRDS_password
```

For Windows:

```
mysqldump --databases database_name ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    -u local_user ^
    -plocal_password | mysql ^
    --host=hostname ^
    --port=3306 ^
    -u RDS_user_name ^
    -pRDS_password
```

Note

Make sure that there isn't a space between the `-p` option and the entered password.

To specify the host name, user name, port, and password to connect to your Amazon RDS DB instance, use the `--host`, `--user` (`-u`), `--port` and `-p` options in the `mysql` command. The host name is the Domain Name Service (DNS) name from the Amazon RDS DB instance endpoint, for example `myinstance.123456789012.us-east-1.rds.amazonaws.com`. You can find the endpoint value in the instance details in the AWS Management Console.

4. Make the source MySQL or MariaDB instance writeable again.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

For more information on making backups for use with replication, see [the MySQL documentation](#).

5. In the AWS Management Console, add the IP address of the server that hosts the external database to the virtual private cloud (VPC) security group for the Amazon RDS DB instance. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the [Amazon Virtual Private Cloud User Guide](#).

The IP address can change when the following conditions are met:

- You are using a public IP address for communication between the external source instance and the DB instance.
- The external source instance was stopped and restarted.

If these conditions are met, verify the IP address before adding it.

You might also need to configure your local network to permit connections from the IP address of your Amazon RDS DB instance. You do this so that your local network can communicate with your

external MySQL or MariaDB instance. To find the IP address of the Amazon RDS DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the Amazon RDS DB instance endpoint.

6. Using the client of your choice, connect to the external instance and create a user to use for replication. Use this account solely for replication and restrict it to your domain to improve security. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. For the external instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Make the Amazon RDS DB instance the replica. To do so, first connect to the Amazon RDS DB instance as the master user. Then identify the external MySQL or MariaDB database as the source instance by using the [mysql.rds_set_external_master \(p. 1441\)](#) command. Use the master log file name and master log position that you determined in step 2. The following is an example.

```
CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306, 'repl_user',  
'password', 'mysql-bin-changelog.000031', 107, 0);
```

Note

On RDS for MySQL, you can choose to use delayed replication by running the [mysql.rds_set_external_master_with_delay \(p. 1443\)](#) stored procedure instead.

On RDS for MySQL, one reason to use delayed replication is to turn on disaster recovery with the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure.

Currently, RDS for MariaDB supports delayed replication but doesn't support the [mysql.rds_start_replication_until](#) procedure.

9. On the Amazon RDS DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

Options for MariaDB database engine

Following, you can find descriptions for options, or additional features, that are available for Amazon RDS instances running the MariaDB DB engine. To turn on these options, you add them to a custom option group, and then associate the option group with your DB instance. For more information about working with option groups, see [Working with option groups \(p. 273\)](#).

Amazon RDS supports the following options for MariaDB:

Option ID	Engine versions
MARIADB_AUDIT_PLUGIN	MariaDB 10.2 and higher

MariaDB Audit Plugin support

Amazon RDS supports using the MariaDB Audit Plugin on MariaDB database instances. The MariaDB Audit Plugin records database activity such as users logging on to the database, queries run against the database, and more. The record of database activity is stored in a log file.

Audit Plugin option settings

Amazon RDS supports the following settings for the MariaDB Audit Plugin option.

Option setting	Valid values	Default value	Description
SERVER_AUDIT_FILESDATABASE	/rdsdbdata/log/audit/	/rdsdbdata/log/audit/	The location of the log file. The log file contains the record of the activity specified in SERVER_AUDIT_EVENTS. For more information, see Viewing and listing database log files (p. 680) and MariaDB database log files (p. 687) .
SERVER_AUDIT_FILESIZELIMIT	1000000000000000		The size in bytes that when reached, causes the file to rotate. For more information, see Log file size (p. 691) .
SERVER_AUDIT_ROTATIONS	9		The number of log rotations to save. For more information, see Log file size (p. 691) and Downloading a database log file (p. 681) .
SERVER_AUDIT_EVENTS	CONNECT, QUERY, TABLE, QUERY_DDL, QUERY_DML, QUERY_DML_NO_SELECT, QUERY_DCL	CONNECT, QUERY	<p>The types of activity to record in the log. Installing the MariaDB Audit Plugin is itself logged.</p> <ul style="list-style-type: none"> CONNECT: Log successful and unsuccessful connections to the database, and disconnections from the database. QUERY: Log the text of all queries run against the database. TABLE: Log tables affected by queries when the queries are run against the database. QUERY_DDL: Similar to the QUERY event, but returns only data definition language (DDL) queries (CREATE, ALTER, and so on).

Option setting	Valid values	Default value	Description
			<ul style="list-style-type: none"> • QUERY_DML: Similar to the QUERY event, but returns only data manipulation language (DML) queries (INSERT, UPDATE, and so on, and also SELECT). • QUERY_DML_NO_SELECT: Similar to the QUERY_DML event, but doesn't log SELECT queries. • QUERY_DCL: Similar to the QUERY event, but returns only data control language (DCL) queries (GRANT, REVOKE, and so on).
SERVER_AUDIT_INCL_USERS	Multiple comma-separated values	None	<p>Include only activity from the specified users. By default, activity is recorded for all users. SERVER_AUDIT_INCL_USERS and SERVER_AUDIT_EXCL_USERS are mutually exclusive. If you add values to SERVER_AUDIT_INCL_USERS, make sure no values are added to SERVER_AUDIT_EXCL_USERS.</p>
SERVER_AUDIT_EXCL_USERS	Multiple comma-separated values	None	<p>Exclude activity from the specified users. By default, activity is recorded for all users. SERVER_AUDIT_INCL_USERS and SERVER_AUDIT_EXCL_USERS are mutually exclusive. If you add values to SERVER_AUDIT_EXCL_USERS, make sure no values are added to SERVER_AUDIT_INCL_USERS.</p> <p>The rdsadmin user queries the database every second to check the health of the database. Depending on your other settings, this activity can possibly cause the size of your log file to grow very large, very quickly. If you don't need to record this activity, add the rdsadmin user to the SERVER_AUDIT_EXCL_USERS list.</p> <p>Note CONNECT activity is always recorded for all users, even if the user is specified for this option setting.</p>
SERVER_AUDIT_LOGGING	ON	ON	<p>Logging is active. The only valid value is ON. Amazon RDS does not support deactivating logging. If you want to deactivate logging, remove the MariaDB Audit Plugin. For more information, see Removing the MariaDB Audit Plugin (p. 1042).</p>
SERVER_AUDIT_QUERYLIMIT	1024		<p>The limit on the length of the query string in a record.</p>

Adding the MariaDB Audit Plugin

The general process for adding the MariaDB Audit Plugin to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

After you add the MariaDB Audit Plugin, you don't need to restart your DB instance. As soon as the option group is active, auditing begins immediately.

To add the MariaDB Audit Plugin

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group. Choose **mariadb** for **Engine**, and choose **10.2** or higher for **Major engine version**. For more information, see [Creating an option group \(p. 274\)](#).
2. Add the **MARIADB_AUDIT_PLUGIN** option to the option group, and configure the option settings. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#). For more information about each setting, see [Audit Plugin option settings \(p. 1040\)](#).
3. Apply the option group to a new or existing DB instance.
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the DB instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Viewing and downloading the MariaDB Audit Plugin log

After you enable the MariaDB Audit Plugin, you access the results in the log files the same way you access any other text-based log files. The audit log files are located at `/rdsdbdata/log/audit/`. For information about viewing the log file in the console, see [Viewing and listing database log files \(p. 680\)](#). For information about downloading the log file, see [Downloading a database log file \(p. 681\)](#).

Modifying MariaDB Audit Plugin settings

After you enable the MariaDB Audit Plugin, you can modify settings for the plugin. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [Audit Plugin option settings \(p. 1040\)](#).

Removing the MariaDB Audit Plugin

Amazon RDS doesn't support turning off logging in the MariaDB Audit Plugin. However, you can remove the plugin from a DB instance. When you remove the MariaDB Audit Plugin, the DB instance is restarted automatically to stop auditing.

To remove the MariaDB Audit Plugin from a DB instance, do one of the following:

- Remove the MariaDB Audit Plugin option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#)
- Modify the DB instance and specify a different option group that doesn't include the plugin. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Parameters for MariaDB

By default, a MariaDB DB instance uses a DB parameter group that is specific to a MariaDB database. This parameter group contains some but not all of the parameters contained in the Amazon RDS DB parameter groups for the MySQL database engine. It also contains a number of new, MariaDB-specific parameters. For information about working with parameter groups and setting parameters, see [Working with parameter groups \(p. 289\)](#).

Viewing MariaDB parameters

RDS for MariaDB parameters are set to the default values of the storage engine that you have selected. For more information about MariaDB parameters, see the [MariaDB documentation](#). For more information about MariaDB storage engines, see [Supported storage engines for MariaDB on Amazon RDS \(p. 979\)](#).

You can view the parameters available for a specific RDS for MariaDB version using the RDS console or the AWS CLI. For information about viewing the parameters in a MariaDB parameter group in the RDS console, see [Viewing parameter values for a DB parameter group \(p. 301\)](#).

Using the AWS CLI, you can view the parameters for an RDS for MariaDB version by running the `describe-engine-default-parameters` command. Specify one of the following values for the `--db-parameter-group-family` option:

- mariadb10.6
- mariadb10.5
- mariadb10.4
- mariadb10.3
- mariadb10.2

For example, to view the parameters for RDS for MariaDB version 10.6, run the following command.

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6
```

Your output looks similar to the following.

```
{  
    "EngineDefaults": {  
        "Parameters": [  
            {  
                "ParameterName": "alter_algorithm",  
                "Description": "Specify the alter table algorithm.",  
                "Source": "engine-default",  
                "ApplyType": "dynamic",  
                "DataType": "string",  
                "AllowedValues": "DEFAULT,COPY,INPLACE,NOCOPY,INSTANT",  
                "IsModifiable": true  
            },  
            {  
                "ParameterName": "analyze_sample_percentage",  
                "Description": "Percentage of rows from the table ANALYZE TABLE will sample  
to collect table statistics.",  
                "Source": "engine-default",  
                "ApplyType": "dynamic",  
                "DataType": "float",  
                "AllowedValues": "0-100",  
                "IsModifiable": true  
            },  
            {  
                "ParameterName": "innodb_max_dirty_pages_pct",  
                "Description": "The percentage of dirty pages that can be stored in memory before  
the InnoDB log writer begins writing them to disk.",  
                "Source": "engine-default",  
                "ApplyType": "dynamic",  
                "DataType": "integer",  
                "AllowedValues": "0-100",  
                "IsModifiable": true  
            }  
        ]  
    }  
}
```

```
{  
    "ParameterName": "aria_block_size",  
    "Description": "Block size to be used for Aria index pages.",  
    "Source": "engine-default",  
    "ApplyType": "static",  
    "DataType": "integer",  
    "AllowedValues": "1024-32768",  
    "IsModifiable": false  
},  
{  
    "ParameterName": "aria_checkpoint_interval",  
    "Description": "Interval in seconds between automatic checkpoints.",  
    "Source": "engine-default",  
    "ApplyType": "dynamic",  
    "DataType": "integer",  
    "AllowedValues": "0-4294967295",  
    "IsModifiable": true  
},  
...  
}
```

To list only the modifiable parameters for RDS for MariaDB version 10.6, run the following command.

For Linux, macOS, or Unix:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6 \  
--query 'EngineDefaults.Parameters[?IsModifiable==`true`]'
```

For Windows:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6 ^  
--query "EngineDefaults.Parameters[?IsModifiable==`true`]"
```

MySQL parameters that aren't available

The following MySQL parameters are not available in MariaDB-specific DB parameter groups:

- bind_address
- binlog_error_action
- binlog_gtid_simple_recovery
- binlog_max_flush_queue_time
- binlog_order_commits
- binlog_row_image
- binlog_rows_query_log_events
- binlogging_impossible_mode
- block_encryption_mode
- core_file
- default_tmp_storage_engine
- div_precision_increment
- end_markers_in_json
- enforce_gtid_consistency
- eq_range_index_dive_limit
- explicit_defaults_for_timestamp
- gtid_executed
- gtid-mode

- gtid_next
- gtid_owned
- gtid_purged
- log_bin_basename
- log_bin_index
- log_bin_use_v1_row_events
- log_slow_admin_statements
- log_slow_slave_statements
- log_throttle_queries_not_using_indexes
- master-info-repository
- optimizer_trace
- optimizer_trace_features
- optimizer_trace_limit
- optimizer_trace_max_mem_size
- optimizer_trace_offset
- relay_log_info_repository
- rpl_stop_slave_timeout
- slave_parallel_workers
- slave_pending_jobs_size_max
- slave_rows_search_algorithms
- storage_engine
- table_open_cache_instances
- timed_mutexes
- transaction_allow_batching
- validate-password
- validate_password_dictionary_file
- validate_password_length
- validate_password_mixed_case_count
- validate_password_number_count
- validate_password_policy
- validate_password_special_char_count

For more information on MySQL parameters, see the [MySQL documentation](#).

Migrating data from a MySQL DB snapshot to a MariaDB DB instance

You can migrate an RDS for MySQL DB snapshot to a new DB instance running MariaDB using the AWS Management Console, the AWS CLI, or Amazon RDS API. You must use a DB snapshot that was created from an Amazon RDS DB instance running MySQL 5.6 or 5.7. To learn how to create an RDS for MySQL DB snapshot, see [Creating a DB snapshot \(p. 448\)](#).

Migrating the snapshot doesn't affect the original DB instance from which the snapshot was taken. You can test and validate the new DB instance before diverting traffic to it as a replacement for the original DB instance.

After you migrate from MySQL to MariaDB, the MariaDB DB instance is associated with the default DB parameter group and option group. After you restore the DB snapshot, you can associate a custom DB parameter group with the new DB instance. However, a MariaDB parameter group has a different set of configurable system variables. For information about the differences between MySQL and MariaDB system variables, see [System Variable Differences between MariaDB and MySQL](#). To learn about DB parameter groups, see [Working with parameter groups \(p. 289\)](#). To learn about option groups, see [Working with option groups \(p. 273\)](#).

Performing the migration

You can migrate an RDS for MySQL DB snapshot to a new MariaDB DB instance using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To migrate a MySQL DB snapshot to a MariaDB DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**, and then select the MySQL DB snapshot you want to migrate.
3. For **Actions**, choose **Migrate snapshot**. The **Migrate database** page appears.
4. For **Migrate to DB Engine**, choose **mariadb**.

Amazon RDS selects the **DB engine version** automatically. You can't change the DB engine version.

The screenshot shows the 'Migrate database' wizard in the AWS RDS console. The top navigation bar includes 'RDS > Snapshots > Migrate snapshot'. The main title is 'Migrate database' with the sub-instruction 'Migrate this database to a new DB engine by selecting your desired options for the migrated instance.' Below this, there are two sections: 'Instance specifications' and 'Settings'. In 'Instance specifications', under 'Migrate to DB engine', the dropdown shows 'mariadb'. Under 'DB engine version', the dropdown shows 'MariaDB 10.5.12'. In the 'Settings' section, there is a link to 'Settings for DB instances (p. 237)'. A vertical sidebar on the right lists 'Next Step' and 'Previous Step' buttons.

5. For the remaining sections, specify your DB instance settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).
6. Choose **Migrate**.

AWS CLI

To migrate data from a MySQL DB snapshot to a MariaDB DB instance, use the AWS CLI `restore-db-instance-from-db-snapshot` command with the following parameters:

- `--db-instance-identifier` – Name of the DB instance to create from the DB snapshot.
- `--db-snapshot-identifier` – The identifier for the DB snapshot to restore from.
- `--engine` – The database engine to use for the new instance.

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-from-db-snapshot \
--db-instance-identifier newmariadbinstance \
--db-snapshot-identifier mysqlsnapshot \
--engine mariadb
```

For Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
--db-instance-identifier newmariadbinstance ^
--db-snapshot-identifier mysqlsnapshot ^
--engine mariadb
```

API

To migrate data from a MySQL DB snapshot to a MariaDB DB instance, call the Amazon RDS API operation [RestoreDBInstanceFromDBSnapshot](#).

Incompatibilities between MariaDB and MySQL

Incompatibilities between MySQL and MariaDB include the following:

- You can't migrate a DB snapshot created with MySQL 8.0 to MariaDB.
- If the source MySQL database uses a SHA256 password hash, make sure to reset user passwords that are SHA256 hashed before you connect to the MariaDB database. The following code shows how to reset a password that is SHA256 hashed.

```
SET old_passwords = 0;
UPDATE mysql.user SET plugin = 'mysql_native_password',
Password = PASSWORD('new_password')
WHERE (User, Host) = ('master_user_name', %);
FLUSH PRIVILEGES;
```

- If your RDS master user account uses the SHA-256 password hash, make sure to reset the password using the AWS Management Console, the [modify-db-instance](#) AWS CLI command, or the [ModifyDBInstance](#) RDS API operation. For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- MariaDB doesn't support the Memcached plugin. However, the data used by the Memcached plugin is stored as InnoDB tables. After you migrate a MySQL DB snapshot, you can access the data used by the Memcached plugin using SQL. For more information about the innodb_memcache database, see [InnoDB memcached Plugin Internals](#).

MariaDB on Amazon RDS SQL reference

Following, you can find descriptions of system stored procedures that are available for Amazon RDS instances running the MariaDB DB engine.

You can use the system stored procedures that are available for MySQL DB instances and MariaDB DB instances. These stored procedures are documented at [MySQL on Amazon RDS SQL reference \(p. 1439\)](#). MariaDB DB instances support all of the stored procedures, except for `mysql.rds_start_replication_until` and `mysql.rds_start_replication_until_gtid`.

Additionally, the following system stored procedures are supported only for Amazon RDS DB instances running MariaDB:

- [mysql.rds_replica_status \(p. 1049\)](#)
- [mysql.rds_set_external_master_gtid \(p. 1050\)](#)
- [mysql.rds_kill_query_id \(p. 1052\)](#)

[mysql.rds_replica_status](#)

Shows the replication status of a MariaDB read replica.

Call this procedure on the read replica to show status information on essential parameters of the replica threads.

Syntax

```
CALL mysql.rds_replica_status;
```

Usage notes

This procedure is only supported for MariaDB DB instances running MariaDB version 10.5 and higher.

This procedure is the equivalent of the `SHOW REPLICA STATUS` command. This command isn't supported for MariaDB version 10.5 and higher DB instances.

In prior versions of MariaDB, the equivalent `SHOW SLAVE STATUS` command required the `REPLICATION SLAVE` privilege. In MariaDB version 10.5 and higher, it requires the `REPLICATION REPLICAR ADMIN` privilege. To protect the RDS management of MariaDB 10.5 and higher DB instances, this new privilege isn't granted to the RDS master user.

Examples

The following example shows the status of a MariaDB read replica:

```
call mysql.rds_replica_status;
```

The response is similar to the following:

```
***** 1. row *****
Replica_IO_State: Waiting for master to send event
Source_Host: XX.XX.XX.XXX
Source_User: rdsrepladmin
Source_Port: 3306
```

```

        Connect_Retry: 60
        Source_Log_File: mysql-bin-changelog.003988
        Read_Source_Log_Pos: 405
            Relay_Log_File: relaylog.011024
            Relay_Log_Pos: 657
        Relay_Source_Log_File: mysql-bin-changelog.003988
            Replica_IO_Running: Yes
            Replica_SQL_Running: Yes
                Replicate_Do_DB:
                Replicate_Ignore_DB:
                Replicate_Do_Table:
                Replicate_Ignore_Table:
        mysql.rds_sysinfo,mysql.rds_history,mysql.rds_replication_status
            Replicate_Wild_Do_Table:
        Replicate_Wild_Ignore_Table:
            Last_Error:
            Skip_Counter: 0
        Exec_Source_Log_Pos: 405
            Relay_Log_Space: 1016
            Until_Condition: None
            Until_Log_File:
            Until_Log_Pos: 0
        Source_SSL_Allowed: No
        Source_SSL_CA_File:
        Source_SSL_CA_Path:
            Source_SSL_Cert:
            Source_SSL_Cipher:
            Source_SSL_Key:
        Seconds_Behind_Master: 0
        Source_SSL_Verify_Server_Cert: No
            Last_IO_Error:
            Last_SQL_Error:
        Replicate_Ignore_Servers:
            Source_Server_Id: 807509301
            Source_SSL_Crl:
            Source_SSL_Crlpath:
                Using_Gtid: Slave_Pos
                Gtid_IO_Pos: 0-807509301-3980
        Replicate_Do_Domain_Ids:
        Replicate_Ignore_Domain_Ids:
            Parallel_Mode: optimistic
            SQL_Delay: 0
            SQL_Remaining_Delay: NULL
        Replica_SQL_Running_State: Reading event from the relay log
            Replica_DDL_Groups: 15
        Replica_Non_Transactional_Groups: 0
            Replica_Transactional_Groups: 3658
1 row in set (0.000 sec)

Query OK, 0 rows affected (0.000 sec)

```

[mysql.rds_set_external_master_gtid](#)

Configures GTID-based replication from a MariaDB instance running external to Amazon RDS to a MariaDB DB instance. This stored procedure is supported only where the external MariaDB instance is version 10.0.24 or higher. When setting up replication where one or both instances do not support MariaDB global transaction identifiers (GTIDs), use [mysql.rds_set_external_master \(p. 1441\)](#).

Using GTIDs for replication provides crash-safety features not offered by binary log replication, so we recommend it in cases where the replicating instances support it.

Syntax

```
CALL mysql.rds_set_external_master_gtid(  
    host_name  
    , host_port  
    , replication_user_name  
    , replication_user_password  
    , gtid  
    , ssl_encryption  
)
```

Parameters

host_name

String. The host name or IP address of the MariaDB instance running external to Amazon RDS that will become the source instance.

host_port

Integer. The port used by the MariaDB instance running external to Amazon RDS to be configured as the source instance. If your network configuration includes SSH port replication that converts the port number, specify the port number that is exposed by SSH.

replication_user_name

String. The ID of a user with REPLICATION SLAVE permissions in the MariaDB DB instance to be configured as the read replica.

replication_user_password

String. The password of the user ID specified in *replication_user_name*.

gtid

String. The global transaction ID on the source instance that replication should start from.

You can use @@gtid_current_pos to get the current GTID if the source instance has been locked while you are configuring replication, so the binary log doesn't change between the points when you get the GTID and when replication starts.

Otherwise, if you are using mysqldump version 10.0.13 or greater to populate the replica instance prior to starting replication, you can get the GTID position in the output by using the --master-data or --dump-slave options. If you are not using mysqldump version 10.0.13 or greater, you can run the SHOW MASTER STATUS or use those same mysqldump options to get the binary log file name and position, then convert them to a GTID by running BINLOG_GTID_POS on the external MariaDB instance:

```
SELECT BINLOG_GTID_POS('<binary log file name>', <binary log file position>);
```

For more information about the MariaDB implementation of GTIDs, go to [Global transaction ID](#) in the MariaDB documentation.

ssl_encryption

A value that specifies whether Secure Socket Layer (SSL) encryption is used on the replication connection. 1 specifies to use SSL encryption, 0 specifies to not use encryption. The default is 0.

Note

The MASTER_SSL_VERIFY_SERVER_CERT option isn't supported. This option is set to 0, which means that the connection is encrypted, but the certificates aren't verified.

Usage notes

The `mysql.rds_set_external_master_gtid` procedure must be run by the master user. It must be run on the MariaDB DB instance that you are configuring as the replica of a MariaDB instance running external to Amazon RDS. Before running `mysql.rds_set_external_master_gtid`, you must have configured the instance of MariaDB running external to Amazon RDS as a source instance. For more information, see [Importing data into a MariaDB DB instance \(p. 1003\)](#).

Warning

Do not use `mysql.rds_set_external_master_gtid` to manage replication between two Amazon RDS DB instances. Use it only when replicating with a MariaDB instance running external to RDS. For information about managing replication between Amazon RDS DB instances, see [Working with read replicas \(p. 370\)](#).

After calling `mysql.rds_set_external_master_gtid` to configure an Amazon RDS DB instance as a read replica, you can call [mysql.rds_start_replication \(p. 1452\)](#) on the replica to start the replication process. You can call [mysql.rds_reset_external_master \(p. 1448\)](#) to remove the read replica configuration.

When `mysql.rds_set_external_master_gtid` is called, Amazon RDS records the time, user, and an action of "set master" in the `mysql.rds_history` and `mysql.rds_replication_status` tables.

Examples

When run on a MariaDB DB instance, the following example configures it as the replica of an instance of MariaDB running external to Amazon RDS.

```
call mysql.rds_set_external_master_gtid
('Sourcedb.some.com',3306,'ReplicationUser','SomePassW0rd','0-123-456',0);
```

mysql.rds_kill_query_id

Ends a query running against the MariaDB server.

Syntax

```
CALL mysql.rds_kill_query_id(queryID);
```

Parameters

queryID

Integer. The identity of the query to be ended.

Usage notes

To stop a query running against the MariaDB server, use the `mysql.rds_kill_query_id` procedure and pass in the ID of that query. To obtain the query ID, query the MariaDB [Information schema PROCESSLIST table](#), as shown following:

```
SELECT USER, HOST, COMMAND, TIME, STATE, INFO, QUERY_ID FROM
INFORMATION_SCHEMA.PROCESSLIST WHERE USER = '<user name>';
```

The connection to the MariaDB server is retained.

Examples

The following example ends a query with a query ID of 230040:

```
call mysql.rds_kill_query_id(230040);
```

Local time zone for MariaDB DB instances

By default, the time zone for a MariaDB DB instance is Universal Time Coordinated (UTC). You can set the time zone for your DB instance to the local time zone for your application instead.

To set the local time zone for a DB instance, set the `time_zone` parameter in the parameter group for your DB instance to one of the supported values listed later in this section. When you set the `time_zone` parameter for a parameter group, all DB instances and read replicas that are using that parameter group change to use the new local time zone. For information on setting parameters in a parameter group, see [Working with parameter groups \(p. 289\)](#).

After you set the local time zone, all new connections to the database reflect the change. If you have any open connections to your database when you change the local time zone, you won't see the local time zone update until after you close the connection and open a new connection.

You can set a different local time zone for a DB instance and one or more of its read replicas. To do this, use a different parameter group for the DB instance and the replica or replicas and set the `time_zone` parameter in each parameter group to a different local time zone.

If you are replicating across AWS Regions, then the source DB instance and the read replica use different parameter groups (parameter groups are unique to an AWS Region). To use the same local time zone for each instance, you must set the `time_zone` parameter in the instance's and read replica's parameter groups.

When you restore a DB instance from a DB snapshot, the local time zone is set to UTC. You can update the time zone to your local time zone after the restore is complete. If you restore a DB instance to a point in time, then the local time zone for the restored DB instance is the time zone setting from the parameter group of the restored DB instance.

You can set your local time zone to one of the following values.

Africa/Cairo	Asia/Riyadh
Africa/Casablanca	Asia/Seoul
Africa/Harare	Asia/Shanghai
Africa/Monrovia	Asia/Singapore
Africa/Nairobi	Asia/Taipei
Africa/Tripoli	Asia/Tehran
Africa/Windhoek	Asia/Tokyo
America/Araguaina	Asia/Ulaanbaatar
America/Asuncion	Asia/Vladivostok
America/Bogota	Asia/Yakutsk
America/Buenos_Aires	Asia/Yerevan
America/Caracas	Atlantic/Azores
America/Chihuahua	Australia/Adelaide
America/Cuiaba	Australia/Brisbane

America/Denver	Australia/Darwin
America/Fortaleza	Australia/Hobart
America/Guatemala	Australia/Perth
America/Halifax	Australia/Sydney
America/Manaus	Brazil/East
America/Matamoros	Canada/Newfoundland
America/Monterrey	Canada/Saskatchewan
America/Montevideo	Canada/Yukon
America/Phoenix	Europe/Amsterdam
America/Santiago	Europe/Athens
America/Tijuana	Europe/Dublin
Asia/Amman	Europe/Helsinki
Asia/Ashgabat	Europe/Istanbul
Asia/Baghdad	Europe/Kaliningrad
Asia/Baku	Europe/Moscow
Asia/Bangkok	Europe/Paris
Asia/Beirut	Europe/Prague
Asia/Calcutta	Europe/Sarajevo
Asia/Damascus	Pacific/Auckland
Asia/Dhaka	Pacific/Fiji
Asia/Irkutsk	Pacific/Guam
Asia/Jerusalem	Pacific/Honolulu
Asia/Kabul	Pacific/Samoa
Asia/Karachi	US/Alaska
Asia/Kathmandu	US/Central
Asia/Krasnoyarsk	US/Eastern
Asia/Magadan	US/East-Indiana
Asia/Muscat	US/Pacific
Asia/Novosibirsk	UTC

RDS for MariaDB limitations

Following are important limitations of using RDS for MariaDB.

Note

This list is not exhaustive.

Topics

- [MariaDB file size limits in Amazon RDS \(p. 1056\)](#)
- [InnoDB reserved word \(p. 1057\)](#)

MariaDB file size limits in Amazon RDS

For MariaDB DB instances, the maximum size of a table is 16 TB when using InnoDB file-per-table tablespaces. This limit also constrains the system tablespace to a maximum size of 16 TB. InnoDB file-per-table tablespaces (with tables each in their own tablespace) are set by default for MariaDB DB instances. This limit isn't related to the maximum storage limit for MariaDB DB instances. For more information about the storage limit, see [Amazon RDS DB instance storage \(p. 64\)](#).

There are advantages and disadvantages to using InnoDB file-per-table tablespaces, depending on your application. To determine the best approach for your application, see [File-per-table tablespaces](#) in the MySQL documentation.

We don't recommend allowing tables to grow to the maximum file size. In general, a better practice is to partition data into smaller tables, which can improve performance and recovery times.

One option that you can use for breaking a large table up into smaller tables is partitioning. *Partitioning* distributes portions of your large table into separate files based on rules that you specify. For example, if you store transactions by date, you can create partitioning rules that distribute older transactions into separate files using partitioning. Then periodically, you can archive the historical transaction data that doesn't need to be readily available to your application. For more information, see [Partitioning](#) in the MySQL documentation.

To determine the file size of a table

Use the following SQL command to determine if any of your tables are too large and are candidates for partitioning. To update table statistics, issue an ANALYZE TABLE command on each table. For more information, see [ANALYZE TABLE statement](#) in the MySQL documentation.

```
SELECT TABLE_SCHEMA, TABLE_NAME,
       round(((DATA_LENGTH + INDEX_LENGTH) / 1024 / 1024), 2) As "Approximate size (MB)",
       DATA_FREE
  FROM information_schema.TABLES
 WHERE TABLE_SCHEMA NOT IN ('mysql', 'information_schema', 'performance_schema');
```

To enable InnoDB file-per-table tablespaces

- To enable InnoDB file-per-table tablespaces, set the `innodb_file_per_table` parameter to `1` in the parameter group for the DB instance.

To disable InnoDB file-per-table tablespaces

- To disable InnoDB file-per-table tablespaces, set the `innodb_file_per_table` parameter to `0` in the parameter group for the DB instance.

For information on updating a parameter group, see [Working with parameter groups \(p. 289\)](#).

When you have enabled or disabled InnoDB file-per-table tablespaces, you can issue an ALTER TABLE command. You can use this command to move a table from the global tablespace to its own tablespace. Or you can move a table from its own tablespace to the global tablespace. Following is an example.

```
ALTER TABLE table_name ENGINE=InnoDB, ALGORITHM=COPY;
```

InnoDB reserved word

InnoDB is a reserved word for RDS for MariaDB. You can't use this name for a MariaDB database.

Amazon RDS for Microsoft SQL Server

Amazon RDS supports several versions and editions of Microsoft SQL Server. The most recent supported version of each major version is listed here. For the full list of supported versions, editions, and RDS engine versions, see [Microsoft SQL Server versions on Amazon RDS \(p. 1066\)](#).

- SQL Server 2019 CU16 15.0.4236.7, released per [KB5014353](#) on June 14, 2022.
- SQL Server 2017 CU30 14.0.3451.2, released per [KB5013756](#) on July 13, 2022.
- SQL Server 2016 SP3 GDR 13.0.6419.1, released per [KB5014355](#) on June 14, 2022.
- SQL Server 2014 SP3 CU4 12.0.6439.10, released per [KB5014164](#) on June 14, 2022.
- SQL Server 2012: It's no longer possible to provision new instances in any Region. Amazon RDS is actively migrating existing instances off this version.
- SQL Server 2008: It's no longer possible to provision new instances in any Region. Amazon RDS is actively migrating existing instances off this version.

For information about licensing for SQL Server, see [Licensing Microsoft SQL Server on Amazon RDS \(p. 1083\)](#). For information about SQL Server builds, see this Microsoft support article about [the latest SQL Server builds](#).

With Amazon RDS, you can create DB instances and DB snapshots, point-in-time restores, and automated or manual backups. DB instances running SQL Server can be used inside a VPC. You can also use Secure Sockets Layer (SSL) to connect to a DB instance running SQL Server, and you can use transparent data encryption (TDE) to encrypt data at rest. Amazon RDS currently supports Multi-AZ deployments for SQL Server using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs) as a high-availability, failover solution.

To deliver a managed service experience, Amazon RDS does not provide shell access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges. Amazon RDS supports access to databases on a DB instance using any standard SQL client application such as Microsoft SQL Server Management Studio. Amazon RDS does not allow direct host access to a DB instance via Telnet, Secure Shell (SSH), or Windows Remote Desktop Connection. When you create a DB instance, the master user is assigned to the `db_owner` role for all user databases on that instance, and has all database-level permissions except for those that are used for backups. Amazon RDS manages backups for you.

Before creating your first DB instance, you should complete the steps in the setting up section of this guide. For more information, see [Setting up for Amazon RDS \(p. 148\)](#).

Topics

- [Common management tasks for Microsoft SQL Server on Amazon RDS \(p. 1059\)](#)
- [Limitations for Microsoft SQL Server DB instances \(p. 1060\)](#)
- [DB instance class support for Microsoft SQL Server \(p. 1062\)](#)
- [Microsoft SQL Server security \(p. 1064\)](#)
- [Compliance program support for Microsoft SQL Server DB instances \(p. 1065\)](#)
- [SSL support for Microsoft SQL Server DB instances \(p. 1066\)](#)
- [Microsoft SQL Server versions on Amazon RDS \(p. 1066\)](#)

- [Version management in Amazon RDS \(p. 1067\)](#)
- [Microsoft SQL Server features on Amazon RDS \(p. 1068\)](#)
- [Change data capture support for Microsoft SQL Server DB instances \(p. 1070\)](#)
- [Features not supported and features with limited support \(p. 1071\)](#)
- [Multi-AZ deployments using Microsoft SQL Server Database Mirroring or Always On availability groups \(p. 1071\)](#)
- [Using Transparent Data Encryption to encrypt data at rest \(p. 1072\)](#)
- [Functions and stored procedures for Amazon RDS for Microsoft SQL Server \(p. 1072\)](#)
- [Local time zone for Microsoft SQL Server DB instances \(p. 1074\)](#)
- [Licensing Microsoft SQL Server on Amazon RDS \(p. 1083\)](#)
- [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#)
- [Updating applications to connect to Microsoft SQL Server DB instances using new SSL/TLS certificates \(p. 1091\)](#)
- [Upgrading the Microsoft SQL Server DB engine \(p. 1094\)](#)
- [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#)
- [Working with read replicas for Microsoft SQL Server in Amazon RDS \(p. 1126\)](#)
- [Multi-AZ deployments for Amazon RDS for Microsoft SQL Server \(p. 1129\)](#)
- [Additional features for Microsoft SQL Server on Amazon RDS \(p. 1134\)](#)
- [Options for the Microsoft SQL Server database engine \(p. 1203\)](#)
- [Common DBA tasks for Microsoft SQL Server \(p. 1291\)](#)

Common management tasks for Microsoft SQL Server on Amazon RDS

The following are the common management tasks you perform with an Amazon RDS for SQL Server DB instance, with links to relevant documentation for each task.

Task area	Relevant documentation
Instance classes, storage, and PIOPS If you are creating a DB instance for production purposes, you should understand how instance classes, storage types, and Provisioned IOPS work in Amazon RDS.	DB instance class support for Microsoft SQL Server (p. 1062) Amazon RDS storage types (p. 64)
Multi-AZ deployments A production DB instance should use Multi-AZ deployments. Multi-AZ deployments provide increased availability, data durability, and fault tolerance for DB instances. Multi-AZ deployments for SQL Server are implemented using SQL Server's native DBM or AGs technology.	Multi-AZ deployments for high availability (p. 121) Multi-AZ deployments using Microsoft SQL Server Database Mirroring or Always On availability groups (p. 1071)
Amazon Virtual Private Cloud (VPC) If your AWS account has a default VPC, then your DB instance is automatically created inside the default VPC. If your account does not have a default VPC, and you want the DB instance in a VPC, you must create the VPC and subnet groups before you create the DB instance.	Working with a DB instance in a VPC (p. 2103)

Task area	Relevant documentation
Security groups By default, DB instances are created with a firewall that prevents access to them. You therefore must create a security group with the correct IP addresses and network configuration to access the DB instance.	Controlling access with security groups (p. 2085)
Parameter groups If your DB instance is going to require specific database parameters, you should create a parameter group before you create the DB instance.	Working with parameter groups (p. 289)
Option groups If your DB instance is going to require specific database options, you should create an option group before you create the DB instance.	Options for the Microsoft SQL Server database engine (p. 1203)
Connecting to your DB instance After creating a security group and associating it to a DB instance, you can connect to the DB instance using any standard SQL client application such as Microsoft SQL Server Management Studio.	Connecting to a DB instance running the Microsoft SQL Server database engine (p. 1084)
Backup and restore When you create your DB instance, you can configure it to take automated backups. You can also back up and restore your databases manually by using full backup files (.bak files).	Working with backups (p. 427) Importing and exporting SQL Server databases using native backup and restore (p. 1099)
Monitoring You can monitor your SQL Server DB instance by using CloudWatch Amazon RDS metrics, events, and enhanced monitoring.	Viewing metrics in the Amazon RDS console (p. 525) Viewing Amazon RDS events (p. 647)
Log files You can access the log files for your SQL Server DB instance.	Monitoring Amazon RDS log files (p. 680) Microsoft SQL Server database log files (p. 696)

There are also advanced administrative tasks for working with SQL Server DB instances. For more information, see the following documentation:

- [Common DBA tasks for Microsoft SQL Server \(p. 1291\)](#).
- [Using Windows Authentication with a SQL Server DB instance \(p. 1143\)](#)
- [Accessing the tempdb database \(p. 1292\)](#)

Limitations for Microsoft SQL Server DB instances

The Amazon RDS implementation of Microsoft SQL Server on a DB instance has some limitations that you should be aware of:

- The maximum number of databases supported on a DB instance depends on the instance class type and the availability mode—Single-AZ, Multi-AZ Database Mirroring (DBM), or Multi-AZ Availability Groups (AGs). The Microsoft SQL Server system databases don't count toward this limit.

The following table shows the maximum number of supported databases for each instance class type and availability mode. Use this table to help you decide if you can move from one instance class type to another, or from one availability mode to another. If your source DB instance has more databases than the target instance class type or availability mode can support, modifying the DB instance fails. You can see the status of your request in the **Events** pane.

Instance class type	Single-AZ	Multi-AZ with DBM	Multi-AZ with Always On AGs
db.*.micro to db.*.medium	30	N/A	N/A
db.*.large	30	30	30
db.*.xlarge to db.*.16xlarge	100	50	75
db.*.24xlarge	100	50	100

* Represents the different instance class types.

For example, let's say that your DB instance runs on a db.*.16xlarge with Single-AZ and that it has 76 databases. You modify the DB instance to upgrade to using Multi-AZ Always On AGs. This upgrade fails, because your DB instance contains more databases than your target configuration can support. If you upgrade your instance class type to db.*.24xlarge instead, the modification succeeds.

If the upgrade fails, you see events and messages similar to the following:

- Unable to modify database instance class. The instance has 76 databases, but after conversion it would only support 75.
- Unable to convert the DB instance to Multi-AZ: The instance has 76 databases, but after conversion it would only support 75.

If the point-in-time restore or snapshot restore fails, you see events and messages similar to the following:

- Database instance put into incompatible-restore. The instance has 76 databases, but after conversion it would only support 75.
- Some ports are reserved for Amazon RDS, and you can't use them when you create a DB instance.
- Client connections from IP addresses within the range 169.254.0.0/16 are not permitted. This is the Automatic Private IP Addressing Range (APIPA), which is used for local-link addressing.
- SQL Server Standard Edition uses only a subset of the available processors if the DB instance has more processors than the software limits (24 cores, 4 sockets, and 128GB RAM). Examples of this are the db.m5.24xlarge and db.r5.24xlarge instance classes.

For more information, see the table of scale limits under [Editions and supported features of SQL Server 2019 \(15.x\)](#) in the Microsoft documentation.

- Amazon RDS for SQL Server doesn't support importing data into the msdb database.
- You can't rename databases on a DB instance in a SQL Server Multi-AZ deployment.
- Make sure that you use these guidelines when setting the following DB parameters on RDS for SQL Server:
 - max server memory (mb) >= 256 MB

- max_worker_threads >= (number of logical CPUs * 7)

For more information on setting DB parameters, see [Working with parameter groups \(p. 289\)](#).

- The maximum storage size for SQL Server DB instances is the following:
 - General Purpose (SSD) storage – 16 TiB for all editions
 - Provisioned IOPS storage – 16 TiB for all editions
 - Magnetic storage – 1 TiB for all editions

If you have a scenario that requires a larger amount of storage, you can use sharding across multiple DB instances to get around the limit. This approach requires data-dependent routing logic in applications that connect to the sharded system. You can use an existing sharding framework, or you can write custom code to enable sharding. If you use an existing framework, the framework can't install any components on the same server as the DB instance.

- The minimum storage size for SQL Server DB instances is the following:
 - General Purpose (SSD) storage – 20 GiB for Enterprise, Standard, Web, and Express Editions
 - Provisioned IOPS storage – 20 GiB for Enterprise, Standard, Web, and Express Editions
 - Magnetic storage – 20 GiB for Enterprise, Standard, Web, and Express Editions
- Amazon RDS doesn't support running these services on the same server as your RDS DB instance:
 - Data Quality Services
 - Master Data Services

To use these features, we recommend that you install SQL Server on an Amazon EC2 instance, or use an on-premises SQL Server instance. In these cases, the EC2 or SQL Server instance acts as the Master Data Services server for your SQL Server DB instance on Amazon RDS. You can install SQL Server on an Amazon EC2 instance with Amazon EBS storage, pursuant to Microsoft licensing policies.

- Because of limitations in Microsoft SQL Server, restoring to a point in time before successfully running `DROP DATABASE` might not reflect the state of that database at that point in time. For example, the dropped database is typically restored to its state up to 5 minutes before the `DROP DATABASE` command was issued. This type of restore means that you can't restore the transactions made during those few minutes on your dropped database. To work around this, you can reissue the `DROP DATABASE` command after the restore operation is completed. Dropping a database removes the transaction logs for that database.
- For SQL Server, you create your databases after you create your DB instance. Database names follow the usual SQL Server naming rules with the following differences:
 - Database names can't start with `rdsadmin`.
 - They can't start or end with a space or a tab.
 - They can't contain any of the characters that create a new line.
 - They can't contain a single quote (').

DB instance class support for Microsoft SQL Server

The computation and memory capacity of a DB instance is determined by its DB instance class. The DB instance class you need depends on your processing power and memory requirements. For more information, see [DB instance classes \(p. 10\)](#).

The following list of DB instance classes supported for Microsoft SQL Server is provided here for your convenience. For the most current list, see the RDS console: <https://console.aws.amazon.com/rds/>.

Not all DB instance classes are available on all supported SQL Server minor versions. For example, some newer DB instance classes such as db.r6i aren't available on older minor versions. You can use the [describe-orderable-db-instance-options](#) AWS CLI command to find out which DB instance classes are available for your SQL Server edition and version.

SQL Server edition	2019 support range	2017 and 2016 support range	2014 support range
	db.r5b.large-db.r5b.4xlarge db.r5d.large-db.r5d.4xlarge db.r6i.large-db.r6i.4xlarge db.m5.large-db.m5.4xlarge db.m5d.large-db.m5d.4xlarge db.m6i.large-db.m6i.4xlarge db.z1d.large-db.z1d.3xlarge db.t3.small-db.t3.xlarge	db.r4.2xlarge db.r5.4xlarge db.r5b.4xlarge db.r5b.5b.large db.r5d.5d.large db.m4.4xlarge db.r6i.4xlarge db.m5.4xlarge db.m5d.4xlarge db.m6i.4xlarge db.m5.2xlarge db.m5d.4xlarge db.m6i.4xlarge db.m5.4xlarge db.m5d.4xlarge db.m6i.4xlarge	db.r3.2xlarge db.r4.2xlarge db.r5.4xlarge db.r5b.5b.large db.r5d.5d.large db.r6i.4xlarge db.r5b.4xlarge db.r5d.4xlarge db.r6i.4xlarge db.r5b.4xlarge db.r5d.4xlarge db.r6i.4xlarge db.r5b.4xlarge db.r5d.4xlarge db.r6i.4xlarge db.r5b.4xlarge db.r5d.4xlarge db.r6i.4xlarge
Express Edition	db.t2.micro-db.t2.medium db.t3.small-db.t3.xlarge	db.t2.micro-db.t2.medium db.t3.small-db.t3.xlarge	db.m3.medium-db.m3.2xlarge db.m4.4xlarge

Microsoft SQL Server security

The Microsoft SQL Server database engine uses role-based security. The master user name that you specify when you create a DB instance is a SQL Server Authentication login that is a member of the processadmin, public, and setupadmin fixed server roles.

Any user who creates a database is assigned to the db_owner role for that database and has all database-level permissions except for those that are used for backups. Amazon RDS manages backups for you.

The following server-level roles aren't available in Amazon RDS for SQL Server:

- bulkadmin
- dbcreator
- diskadmin
- securityadmin
- serveradmin
- sysadmin

The following server-level permissions aren't available on RDS for SQL Server DB instances:

- ALTER ANY DATABASE
- ALTER ANY EVENT NOTIFICATION
- ALTER RESOURCES

- ALTER SETTINGS (you can use the DB parameter group API operations to modify parameters; for more information, see [Working with parameter groups \(p. 289\)](#))
- AUTHENTICATE SERVER
- CONTROL_SERVER
- CREATE DDL EVENT NOTIFICATION
- CREATE ENDPOINT
- CREATE SERVER ROLE
- CREATE TRACE EVENT NOTIFICATION
- DROP ANY DATABASE
- EXTERNAL ACCESS ASSEMBLY
- SHUTDOWN (You can use the RDS reboot option instead)
- UNSAFE ASSEMBLY
- ALTER ANY AVAILABILITY GROUP
- CREATE ANY AVAILABILITY GROUP

Compliance program support for Microsoft SQL Server DB instances

AWS Services in scope have been fully assessed by a third-party auditor and result in a certification, attestation of compliance, or Authority to Operate (ATO). For more information, see [AWS services in scope by compliance program](#).

HIPAA support for Microsoft SQL Server DB instances

You can use Amazon RDS for Microsoft SQL Server databases to build HIPAA-compliant applications. You can store healthcare-related information, including protected health information (PHI), under a Business Associate Agreement (BAA) with AWS. For more information, see [HIPAA compliance](#).

Amazon RDS for SQL Server supports HIPAA for the following versions and editions:

- SQL Server 2019 Enterprise, Standard, and Web Editions
- SQL Server 2017 Enterprise, Standard, and Web Editions
- SQL Server 2016 Enterprise, Standard, and Web Editions
- SQL Server 2014 Enterprise, Standard, and Web Editions

To enable HIPAA support on your DB instance, set up the following three components.

Component	Details
Auditing	To set up auditing, set the parameter <code>rds.sqlserver_audit</code> to the value <code>fedramp_hipaa</code> . If your DB instance is not already using a custom DB parameter group, you must create a custom parameter group and attach it to your DB instance before you can modify the <code>rds.sqlserver_audit</code> parameter. For more information, see Working with parameter groups (p. 289) .
Transport encryption	To set up transport encryption, force all connections to your DB instance to use Secure Sockets Layer (SSL). For more information, see Forcing connections to your DB instance to use SSL (p. 1135) .

Component	Details
Encryption at rest	<p>To set up encryption at rest, you have two options:</p> <ol style="list-style-type: none"> If you're running SQL Server 2014–2019 Enterprise Edition or 2019 Standard Edition, you can use Transparent Data Encryption (TDE) to achieve encryption at rest. For more information, see Support for Transparent Data Encryption in SQL Server (p. 1217). You can set up encryption at rest by using AWS Key Management Service (AWS KMS) encryption keys. For more information, see Encrypting Amazon RDS resources (p. 2000).

SSL support for Microsoft SQL Server DB instances

You can use SSL to encrypt connections between your applications and your Amazon RDS DB instances running Microsoft SQL Server. You can also force all connections to your DB instance to use SSL. If you force connections to use SSL, it happens transparently to the client, and the client doesn't have to do any work to use SSL.

SSL is supported in all AWS Regions and for all supported SQL Server editions. For more information, see [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#).

Microsoft SQL Server versions on Amazon RDS

You can specify any currently supported Microsoft SQL Server version when creating a new DB instance. You can specify the Microsoft SQL Server major version (such as Microsoft SQL Server 14.00), and any supported minor version for the specified major version. If no version is specified, Amazon RDS defaults to a supported version, typically the most recent version. If a major version is specified but a minor version is not, Amazon RDS defaults to a recent release of the major version you have specified.

The following table shows the supported versions for all editions and all AWS Regions, except where noted. You can also use the `describe-db-engine-versions` AWS CLI command to see a list of supported versions, as well as defaults for newly created DB instances.

SQL Server versions supported in RDS

Major version	Minor version	RDS API EngineVersion and CLI engine-version
SQL Server 2019	15.00.4236.7 (CU16)	15.00.4236.7.v1
	15.00.4198.2 (CU15)	15.00.4198.2.v1
	15.00.4153.1 (CU12)	15.00.4153.1.v1
	15.00.4073.23 (CU8)	15.00.4073.23.v1
	15.00.4043.16 (CU5)	15.00.4043.16.v1
SQL Server 2017	14.00.3451.2 (CU30)	14.00.3451.2.v1
	14.00.3421.10 (CU27)	14.00.3421.10.v1
	14.00.3401.7 (CU25)	14.00.3401.7.v1
	14.00.3381.3 (CU23)	14.00.3381.3.v1

Major version	Minor version	RDS API EngineVersion and CLI engine-version
	14.00.3356.20 (CU22)	14.00.3356.20.v1
	14.00.3294.2 (CU20)	14.00.3294.2.v1
	14.00.3281.6 (CU19)	14.00.3281.6.v1
SQL Server 2016	13.00.6419.1 (SP3 + Hotfix)	13.00.6419.1.v1
	13.00.6300.2 (SP3)	13.00.6300.2.v1
SQL Server 2014	12.00.6439.10 (SP3 CU4 SU)	12.00.6439.10.v1
	12.00.6433.1 (SP3 CU4 SU)	12.00.6433.1.v1
	12.00.6329.1 (SP3 CU4)	12.00.6329.1.v1
	12.00.6293.0 (SP3 CU3)	12.00.6293.0.v1

Version management in Amazon RDS

Amazon RDS includes flexible version management that enables you to control when and how your DB instance is patched or upgraded. This enables you to do the following for your DB engine:

- Maintain compatibility with database engine patch versions.
- Test new patch versions to verify that they work with your application before you deploy them in production.
- Plan and perform version upgrades to meet your service level agreements and timing requirements.

Microsoft SQL Server engine patching in Amazon RDS

Amazon RDS periodically aggregates official Microsoft SQL Server database patches into a DB instance engine version that's specific to Amazon RDS. For more information about the Microsoft SQL Server patches in each engine version, see [Version and feature support on Amazon RDS](#).

Currently, you manually perform all engine upgrades on your DB instance. For more information, see [Upgrading the Microsoft SQL Server DB engine \(p. 1094\)](#).

Deprecation schedule for major engine versions of Microsoft SQL Server on Amazon RDS

The following table displays the planned schedule of deprecations for major engine versions of Microsoft SQL Server.

Date	Information
July 12, 2022	Microsoft will stop critical patch updates for SQL Server 2012. For more information, see Documentation .
June 1, 2022	Amazon RDS plans to end support of Microsoft SQL Server 2012 on RDS for SQL Server. It is scheduled to migrate to SQL Server 2014 (latest minor version available). For more information, see Server ending support for SQL Server 2012 major versions .

Date	Information
	To avoid an automatic upgrade from Microsoft SQL Server 2012, you can upgrade at a time, see Upgrading a DB instance engine version (p. 360) .
September 1, 2021	Amazon RDS is starting to disable the creation of new RDS for SQL Server DB instances using Microsoft SQL Server 2008R2. For more information, see Announcement: Amazon RDS for SQL Server ending support for SQL Server 2008R2 (p. 360) .
July 12, 2019	The Amazon RDS team deprecated support for Microsoft SQL Server 2008 R2 in June 2019. Microsoft SQL Server 2008 R2 are migrating to SQL Server 2012 (latest minor version available). To avoid an automatic upgrade from Microsoft SQL Server 2008 R2, you can upgrade at a time, see Upgrading a DB instance engine version (p. 360) .
April 25, 2019	Before the end of April 2019, you will no longer be able to create new Amazon RDS for SQL Server 2008R2.

Microsoft SQL Server features on Amazon RDS

The supported SQL Server versions on Amazon RDS include the following features. In general, a version also includes features from the previous versions, unless otherwise noted in the Microsoft documentation.

Topics

- [Microsoft SQL Server 2019 features \(p. 1068\)](#)
- [Microsoft SQL Server 2017 features \(p. 1069\)](#)
- [Microsoft SQL Server 2016 features \(p. 1069\)](#)
- [Microsoft SQL Server 2014 features \(p. 1069\)](#)
- [Microsoft SQL Server 2012 end of support on Amazon RDS \(p. 1070\)](#)
- [Microsoft SQL Server 2008 R2 end of support on Amazon RDS \(p. 1070\)](#)

Microsoft SQL Server 2019 features

SQL Server 2019 includes many new features, such as the following:

- Accelerated database recovery (ADR) – Reduces crash recovery time after a restart or a long-running transaction rollback.
- Intelligent Query Processing (IQP):
 - Row mode memory grant feedback – Corrects excessive grants automatically, that would otherwise result in wasted memory and reduced concurrency.
 - Batch mode on rowstore – Enables batch mode execution for analytic workloads without requiring columnstore indexes.
 - Table variable deferred compilation – Improves plan quality and overall performance for queries that reference table variables.
- Intelligent performance:
 - `OPTIMIZE_FOR_SEQUENTIAL_KEY` index option – Improves throughput for high-concurrency inserts into indexes.
 - Improved indirect checkpoint scalability – Helps databases with heavy DML workloads.
 - Concurrent Page Free Space (PFS) updates – Enables handling as a shared latch rather than an exclusive latch.

- Monitoring improvements:
 - WAIT_ON_SYNC_STATISTICS_REFRESH wait type – Shows accumulated instance-level time spent on synchronous statistics refresh operations.
 - Database-scoped configurations – Include LIGHTWEIGHT_QUERY_PROFILING and LAST_QUERY_PLAN_STATS.
 - Dynamic management functions (DMFs) – Include sys.dm_exec_query_plan_stats and sys.dm_db_page_info.
- Verbose truncation warnings – The data truncation error message defaults to include table and column names and the truncated value.
- Resumable online index creation – In SQL Server 2017, only resumable online index rebuild is supported.

For the full list of SQL Server 2019 features, see [What's new in SQL Server 2019 \(15.x\)](#) in the Microsoft documentation.

For a list of unsupported features, see [Features not supported and features with limited support \(p. 1071\)](#).

Microsoft SQL Server 2017 features

SQL Server 2017 includes many new features, such as the following:

- Adaptive query processing
- Automatic plan correction (an automatic tuning feature)
- GraphDB
- Resumable index rebuilds

For the full list of SQL Server 2017 features, see [What's new in SQL Server 2017](#) in the Microsoft documentation.

For a list of unsupported features, see [Features not supported and features with limited support \(p. 1071\)](#).

Microsoft SQL Server 2016 features

Amazon RDS supports the following features of SQL Server 2016:

- Always Encrypted
- JSON Support
- Operational Analytics
- Query Store
- Temporal Tables

For the full list of SQL Server 2016 features, see [What's new in SQL Server 2016](#) in the Microsoft documentation.

Microsoft SQL Server 2014 features

In addition to supported features of SQL Server 2012, Amazon RDS supports the new query optimizer available in SQL Server 2014, and also the delayed durability feature.

For a list of unsupported features, see [Features not supported and features with limited support \(p. 1071\)](#).

SQL Server 2014 supports all the parameters from SQL Server 2012 and uses the same default values. SQL Server 2014 includes one new parameter, backup checksum default. For more information, see [How to enable the CHECKSUM option if backup utilities do not expose the option](#) in the Microsoft documentation.

Microsoft SQL Server 2012 end of support on Amazon RDS

SQL Server 2012 has reached its end of support on Amazon RDS.

RDS is upgrading all existing DB instances that are still using SQL Server 2012 to the latest minor version of SQL Server 2014. For more information, see [Version management in Amazon RDS \(p. 1067\)](#).

Microsoft SQL Server 2008 R2 end of support on Amazon RDS

SQL Server 2008 R2 has reached its end of support on Amazon RDS.

RDS is upgrading all existing DB instances that are still using SQL Server 2008 R2 to the latest minor version of SQL Server 2012. For more information, see [Version management in Amazon RDS \(p. 1067\)](#).

Change data capture support for Microsoft SQL Server DB instances

Amazon RDS supports change data capture (CDC) for your DB instances running Microsoft SQL Server. CDC captures changes that are made to the data in your tables, and stores metadata about each change that you can access later. For more information, see [Change data capture](#) in the Microsoft documentation.

Amazon RDS supports CDC for the following SQL Server editions and versions:

- Microsoft SQL Server Enterprise Edition (All versions)
- Microsoft SQL Server Standard Edition:
 - 2019
 - ea
 - 2017
 - 2016 version 13.00.4422.0 SP1 CU2 and later

To use CDC with your Amazon RDS DB instances, first enable or disable CDC at the database level by using RDS-provided stored procedures. After that, any user that has the db_owner role for that database can use the native Microsoft stored procedures to control CDC on that database. For more information, see [Using change data capture \(p. 1303\)](#).

You can use CDC and AWS Database Migration Service to enable ongoing replication from SQL Server DB instances.

Features not supported and features with limited support

The following Microsoft SQL Server features aren't supported on Amazon RDS:

- Backing up to Microsoft Azure Blob Storage
- Buffer pool extension
- Custom password policies
- Data Quality Services
- Database Log Shipping
- Database snapshots (Amazon RDS supports only DB instance snapshots)
- Extended stored procedures, including `xp_cmdshell`
- FILESTREAM support
- File tables
- Machine Learning and R Services (requires OS access to install it)
- Maintenance plans
- Performance Data Collector
- Policy-Based Management
- PolyBase
- Replication
- Resource Governor
- Server-level triggers
- Service Broker endpoints
- Stretch database
- TRUSTWORTHY database property (requires sysadmin role)
- T-SQL endpoints (all operations using CREATE ENDPOINT are unavailable)
- WCF Data Services

The following Microsoft SQL Server features have limited support on Amazon RDS:

- Distributed queries/linked servers. For more information, see [Implement linked servers with Amazon RDS for Microsoft SQL Server](#).
- Common Runtime Language (CLR). On RDS for SQL Server 2016 and lower versions, CLR is supported in SAFE mode and using assembly bits only. CLR isn't supported on RDS for SQL Server 2017 and higher versions. For more information, see [Common Runtime Language Integration](#) in the Microsoft documentation.

Multi-AZ deployments using Microsoft SQL Server Database Mirroring or Always On availability groups

Amazon RDS supports Multi-AZ deployments for DB instances running Microsoft SQL Server by using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). Multi-AZ deployments provide increased availability, data durability, and fault tolerance for DB instances. In the event of planned database maintenance or unplanned service disruption, Amazon RDS automatically fails

over to the up-to-date secondary replica so database operations can resume quickly without manual intervention. The primary and secondary instances use the same endpoint, whose physical network address transitions to the passive secondary replica as part of the failover process. You don't have to reconfigure your application when a failover occurs.

Amazon RDS manages failover by actively monitoring your Multi-AZ deployment and initiating a failover when a problem with your primary occurs. Failover doesn't occur unless the standby and primary are fully in sync. Amazon RDS actively maintains your Multi-AZ deployment by automatically repairing unhealthy DB instances and re-establishing synchronous replication. You don't have to manage anything. Amazon RDS handles the primary, the witness, and the standby instance for you. When you set up SQL Server Multi-AZ, RDS configures passive secondary instances for all of the databases on the instance.

For more information, see [Multi-AZ deployments for Amazon RDS for Microsoft SQL Server \(p. 1129\)](#).

Using Transparent Data Encryption to encrypt data at rest

Amazon RDS supports Microsoft SQL Server Transparent Data Encryption (TDE), which transparently encrypts stored data. Amazon RDS uses option groups to enable and configure these features. For more information about the TDE option, see [Support for Transparent Data Encryption in SQL Server \(p. 1217\)](#).

Functions and stored procedures for Amazon RDS for Microsoft SQL Server

Following, you can find a list of the Amazon RDS functions and stored procedures that help automate SQL Server tasks.

Task type	Procedure or function	Where it's used
Administrative tasks	rds_drop_database	Dropping a Microsoft SQL Server database (p. 1301)
	rds_failover_time	Determining the last failover time (p. 1300)
	rds_modify_db_name	Renaming a Microsoft SQL Server database in a Multi-AZ deployment (p. 1301)
	rds_read_error_log	Viewing error and agent logs (p. 1308)
	rds_set_config	This operation is used to set various DB instance configurations: <ul style="list-style-type: none">• Change data capture for Multi-AZ instances (p. 1304)• Setting the retention period for trace and dump files (p. 1309)• Compressing backup files (p. 1115)
	rds_set_database_online	Transitioning a Microsoft SQL Server database from OFFLINE to ONLINE (p. 1303)
	rds_set_system_table_as_cte	Transferring SQL Server Agent job replication (p. 1306)
	rds_fn_get_system_database_sync_objects	
	rds_fn_server_object_last_sync_time	

Task type	Procedure or function	Where it's used
	rds_show_configuration	Shows the values that are set using <code>rds_set_configuration</code> , see these topics: <ul style="list-style-type: none"> Change data capture for Multi-AZ instances (p. 1304) Setting the retention period for trace and dump files (p. 1309)
	rds_shrink_tempdb	Shrinking the tempdb database (p. 1292)
Change data capture (CDC)	rds_cdc_disable	Disabling CDC (p. 1303)
	rds_cdc_enable	Enabling CDC (p. 1303)
Database Mail	rds_fn_sysmail_viewitem	Viewing messages, logs, and attachments (p. 1175)
	rds_fn_sysmail_viewmsg	Viewing messages, logs, and attachments (p. 1175)
	rds_fn_sysmail_viewattachment	Viewing attachments, logs, and attachments (p. 1175)
	rds_sysmail_configure	This operation is used in starting and stopping the mail queue: <ul style="list-style-type: none"> Starting the mail queue (p. 1176) Stopping the mail queue (p. 1176)
	rds_sysmail_deleteitems	Deleting items (sp1175)
Native backup and restore	rds_backup_database	Backing up a database (p. 1105)
	rds_cancel_task	Canceling a task (p. 1112)
	rds_finish_restore	Finishing a database restore (p. 1111)
	rds_restore_database	Restoring a database (p. 1108)
	rds_restore_log	Restoring a log (p. 1110)
Amazon S3 file transfer	rds_delete_from_file_system	Deleting files on the RDS DB instance (p. 1162)
	rds_download_from_s3	Downloading files from an Amazon S3 bucket to a SQL Server DB instance (p. 1160)
	rds_gather_file_list	Listing files on the RDS DB instance (p. 1162)
	rds_upload_to_s3	Uploading files from a SQL Server DB instance to an Amazon S3 bucket (p. 1161)
Microsoft Distributed Transaction Coordinator (MSDTC)	rds_msdtc_transaction_start_tracing	Starting tracing (p. 1287)
SQL Server Audit	rds_fn_get_audit_file	Viewing audit logs (p. 1227)
Transparent Data Encryption	rds_backup_tde_certificate	Sign certificate
	rds_drop_tde_certificate	Transparent Data Encryption in SQL Server (p. 1217)
	rds_restore_tde_certificate	
	rds_fn_list_user_tde_certificates	

Task type	Procedure or function	Where it's used
Microsoft Business Intelligence (MSBI)	rds_msbi_task	<p>This operation is used with SQL Server Analysis Services (SSAS):</p> <ul style="list-style-type: none"> • Deploying SSAS projects on Amazon RDS (p. 1237) • Adding a domain user as a database administrator (p. 1241) • Backing up an SSAS database (p. 1245) • Restoring an SSAS database (p. 1245) <p>This operation is also used with SQL Server Integration Services (SSIS):</p> <ul style="list-style-type: none"> • Administrative permissions on SSISDB (p. 1258) • Deploying an SSIS project (p. 1259) <p>This operation is also used with SQL Server Reporting Services (SSRS):</p> <ul style="list-style-type: none"> • Granting access to domain users (p. 1272) • Revoking system-level permissions (p. 1275)
	rds_fn_task_status	<p>This operation shows the status of MSBI tasks:</p> <ul style="list-style-type: none"> • SSAS: Monitoring the status of a deployment task (p. 1238) • SSIS: Monitoring the status of a deployment task (p. 1260) • SSRS: Monitoring the status of a task (p. 1275)
SSIS	rds_drop_ssis_database	Delete the SSISDB database (p. 1265)
	rds_sqlagent_proxy	Create an SSIS proxy (p. 1262)
SSRS	rds_drop_ssrs_database	Delete the SSRS databases (p. 1277)

Local time zone for Microsoft SQL Server DB instances

The time zone of an Amazon RDS DB instance running Microsoft SQL Server is set by default. The current default is Coordinated Universal Time (UTC). You can set the time zone of your DB instance to a local time zone instead, to match the time zone of your applications.

You set the time zone when you first create your DB instance. You can create your DB instance by using the [AWS Management Console](#), the Amazon RDS API [CreateDBInstance](#) action, or the AWS CLI [create-db-instance](#) command.

If your DB instance is part of a Multi-AZ deployment (using SQL Server DBM or AGs), then when you fail over, your time zone remains the local time zone that you set. For more information, see [Multi-AZ deployments using Microsoft SQL Server Database Mirroring or Always On availability groups \(p. 1071\)](#).

When you request a point-in-time restore, you specify the time to restore to. The time is shown in your local time zone. For more information, see [Restoring a DB instance to a specified time \(p. 499\)](#).

The following are limitations to setting the local time zone on your DB instance:

- You can't modify the time zone of an existing SQL Server DB instance.
- You can't restore a snapshot from a DB instance in one time zone to a DB instance in a different time zone.
- We strongly recommend that you don't restore a backup file from one time zone to a different time zone. If you restore a backup file from one time zone to a different time zone, you must audit your queries and applications for the effects of the time zone change. For more information, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Supported time zones

You can set your local time zone to one of the values listed in the following table.

Time zones supported for Amazon RDS on SQL Server

Time zone	Standard time offset	Description	Notes
Afghanistan Standard Time	(UTC+04:30)	Kabul	This time zone doesn't observe daylight saving time.
Alaskan Standard Time	(UTC−09:00)	Alaska	
Aleutian Standard Time	(UTC−10:00)	Aleutian Islands	
Altai Standard Time	(UTC+07:00)	Barnaul, Gorno-Altaysk	
Arab Standard Time	(UTC+03:00)	Kuwait, Riyadh	This time zone doesn't observe daylight saving time.
Arabian Standard Time	(UTC+04:00)	Abu Dhabi, Muscat	
Arabic Standard Time	(UTC+03:00)	Baghdad	This time zone doesn't observe daylight saving time.
Argentina Standard Time	(UTC−03:00)	City of Buenos Aires	This time zone doesn't observe daylight saving time.
Astrakhan Standard Time	(UTC+04:00)	Astrakhan, Ulyanovsk	
Atlantic Standard Time	(UTC−04:00)	Atlantic Time (Canada)	
AUS Central Standard Time	(UTC+09:30)	Darwin	This time zone doesn't observe daylight saving time.
Aus Central W. Standard Time	(UTC+08:45)	Eucla	
AUS Eastern Standard Time	(UTC+10:00)	Canberra, Melbourne, Sydney	
Azerbaijan Standard Time	(UTC+04:00)	Baku	
Azores Standard Time	(UTC−01:00)	Azores	

Time zone	Standard time offset	Description	Notes
Bahia Standard Time	(UTC-03:00)	Salvador	
Bangladesh Standard Time	(UTC+06:00)	Dhaka	This time zone doesn't observe daylight saving time.
Belarus Standard Time	(UTC+03:00)	Minsk	This time zone doesn't observe daylight saving time.
Bougainville Standard Time	(UTC+11:00)	Bougainville Island	
Canada Central Standard Time	(UTC-06:00)	Saskatchewan	This time zone doesn't observe daylight saving time.
Cape Verde Standard Time	(UTC-01:00)	Cabo Verde Is.	This time zone doesn't observe daylight saving time.
Caucasus Standard Time	(UTC+04:00)	Yerevan	
Cen. Australia Standard Time	(UTC+09:30)	Adelaide	
Central America Standard Time	(UTC-06:00)	Central America	This time zone doesn't observe daylight saving time.
Central Asia Standard Time	(UTC+06:00)	Astana	This time zone doesn't observe daylight saving time.
Central Brazilian Standard Time	(UTC-04:00)	Cuiaba	
Central Europe Standard Time	(UTC+01:00)	Belgrade, Bratislava, Budapest, Ljubljana, Prague	
Central European Standard Time	(UTC+01:00)	Sarajevo, Skopje, Warsaw, Zagreb	
Central Pacific Standard Time	(UTC+11:00)	Solomon Islands, New Caledonia	This time zone doesn't observe daylight saving time.
Central Standard Time	(UTC-06:00)	Central Time (US and Canada)	
Central Standard Time (Mexico)	(UTC-06:00)	Guadalajara, Mexico City, Monterrey	
Chatham Islands Standard Time	(UTC+12:45)	Chatham Islands	
China Standard Time	(UTC+08:00)	Beijing, Chongqing, Hong Kong, Urumqi	This time zone doesn't observe daylight saving time.

Time zone	Standard time offset	Description	Notes
Cuba Standard Time	(UTC-05:00)	Havana	
Dateline Standard Time	(UTC-12:00)	International Date Line West	This time zone doesn't observe daylight saving time.
E. Africa Standard Time	(UTC+03:00)	Nairobi	This time zone doesn't observe daylight saving time.
E. Australia Standard Time	(UTC+10:00)	Brisbane	This time zone doesn't observe daylight saving time.
E. Europe Standard Time	(UTC+02:00)	Chisinau	
E. South America Standard Time	(UTC-03:00)	Brasilia	
Easter Island Standard Time	(UTC-06:00)	Easter Island	
Eastern Standard Time	(UTC-05:00)	Eastern Time (US and Canada)	
Eastern Standard Time (Mexico)	(UTC-05:00)	Chetumal	
Egypt Standard Time	(UTC+02:00)	Cairo	
Ekaterinburg Standard Time	(UTC+05:00)	Ekaterinburg	
Fiji Standard Time	(UTC+12:00)	Fiji	
FLE Standard Time	(UTC+02:00)	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	
Georgian Standard Time	(UTC+04:00)	Tbilisi	This time zone doesn't observe daylight saving time.
GMT Standard Time	(UTC)	Dublin, Edinburgh, Lisbon, London	This time zone isn't the same as Greenwich Mean Time. This time zone does observe daylight saving time.
Greenland Standard Time	(UTC-03:00)	Greenland	
Greenwich Standard Time	(UTC)	Monrovia, Reykjavik	This time zone doesn't observe daylight saving time.
GTB Standard Time	(UTC+02:00)	Athens, Bucharest	
Haiti Standard Time	(UTC-05:00)	Haiti	
Hawaiian Standard Time	(UTC-10:00)	Hawaii	

Time zone	Standard time offset	Description	Notes
India Standard Time	(UTC+05:30)	Chennai, Kolkata, Mumbai, New Delhi	This time zone doesn't observe daylight saving time.
Iran Standard Time	(UTC+03:30)	Tehran	
Israel Standard Time	(UTC+02:00)	Jerusalem	
Jordan Standard Time	(UTC+02:00)	Amman	
Kaliningrad Standard Time	(UTC+02:00)	Kaliningrad	
Kamchatka Standard Time	(UTC+12:00)	Petropavlovsk-Kamchatsky – Old	
Korea Standard Time	(UTC+09:00)	Seoul	This time zone doesn't observe daylight saving time.
Libya Standard Time	(UTC+02:00)	Tripoli	
Line Islands Standard Time	(UTC+14:00)	Kiritimati Island	
Lord Howe Standard Time	(UTC+10:30)	Lord Howe Island	
Magadan Standard Time	(UTC+11:00)	Magadan	This time zone doesn't observe daylight saving time.
Magallanes Standard Time	(UTC–03:00)	Punta Arenas	
Marquesas Standard Time	(UTC–09:30)	Marquesas Islands	
Mauritius Standard Time	(UTC+04:00)	Port Louis	This time zone doesn't observe daylight saving time.
Middle East Standard Time	(UTC+02:00)	Beirut	
Montevideo Standard Time	(UTC–03:00)	Montevideo	
Morocco Standard Time	(UTC+01:00)	Casablanca	
Mountain Standard Time	(UTC–07:00)	Mountain Time (US and Canada)	
Mountain Standard Time (Mexico)	(UTC–07:00)	Chihuahua, La Paz, Mazatlan	
Myanmar Standard Time	(UTC+06:30)	Yangon (Rangoon)	This time zone doesn't observe daylight saving time.
N. Central Asia Standard Time	(UTC+07:00)	Novosibirsk	
Namibia Standard Time	(UTC+02:00)	Windhoek	

Time zone	Standard time offset	Description	Notes
Nepal Standard Time	(UTC+05:45)	Kathmandu	This time zone doesn't observe daylight saving time.
New Zealand Standard Time	(UTC+12:00)	Auckland, Wellington	
Newfoundland Standard Time	(UTC−03:30)	Newfoundland	
Norfolk Standard Time	(UTC+11:00)	Norfolk Island	
North Asia East Standard Time	(UTC+08:00)	Irkutsk	
North Asia Standard Time	(UTC+07:00)	Krasnoyarsk	
North Korea Standard Time	(UTC+09:00)	Pyongyang	
Omsk Standard Time	(UTC+06:00)	Omsk	
Pacific SA Standard Time	(UTC−03:00)	Santiago	
Pacific Standard Time	(UTC−08:00)	Pacific Time (US and Canada)	
Pacific Standard Time (Mexico)	(UTC−08:00)	Baja California	
Pakistan Standard Time	(UTC+05:00)	Islamabad, Karachi	This time zone doesn't observe daylight saving time.
Paraguay Standard Time	(UTC−04:00)	Asuncion	
Romance Standard Time	(UTC+01:00)	Brussels, Copenhagen, Madrid, Paris	
Russia Time Zone 10	(UTC+11:00)	Chokurdakh	
Russia Time Zone 11	(UTC+12:00)	Anadyr, Petropavlovsk-Kamchatsky	
Russia Time Zone 3	(UTC+04:00)	Izhevsk, Samara	
Russian Standard Time	(UTC+03:00)	Moscow, St. Petersburg, Volgograd	This time zone doesn't observe daylight saving time.
SA Eastern Standard Time	(UTC−03:00)	Cayenne, Fortaleza	This time zone doesn't observe daylight saving time.
SA Pacific Standard Time	(UTC−05:00)	Bogota, Lima, Quito, Rio Branco	This time zone doesn't observe daylight saving time.
SA Western Standard Time	(UTC−04:00)	Georgetown, La Paz, Manaus, San Juan	This time zone doesn't observe daylight saving time.

Time zone	Standard time offset	Description	Notes
Saint Pierre Standard Time	(UTC-03:00)	Saint Pierre and Miquelon	
Sakhalin Standard Time	(UTC+11:00)	Sakhalin	
Samoa Standard Time	(UTC+13:00)	Samoa	
Sao Tome Standard Time	(UTC+01:00)	Sao Tome	
Saratov Standard Time	(UTC+04:00)	Saratov	
SE Asia Standard Time	(UTC+07:00)	Bangkok, Hanoi, Jakarta	This time zone doesn't observe daylight saving time.
Singapore Standard Time	(UTC+08:00)	Kuala Lumpur, Singapore	This time zone doesn't observe daylight saving time.
South Africa Standard Time	(UTC+02:00)	Harare, Pretoria	This time zone doesn't observe daylight saving time.
Sri Lanka Standard Time	(UTC+05:30)	Sri Jayawardenepura	This time zone doesn't observe daylight saving time.
Sudan Standard Time	(UTC+02:00)	Khartoum	
Syria Standard Time	(UTC+02:00)	Damascus	
Taipei Standard Time	(UTC+08:00)	Taipei	This time zone doesn't observe daylight saving time.
Tasmania Standard Time	(UTC+10:00)	Hobart	
Tocantins Standard Time	(UTC-03:00)	Araguaina	
Tokyo Standard Time	(UTC+09:00)	Osaka, Sapporo, Tokyo	This time zone doesn't observe daylight saving time.
Tomsk Standard Time	(UTC+07:00)	Tomsk	
Tonga Standard Time	(UTC+13:00)	Nuku'alofa	This time zone doesn't observe daylight saving time.
Transbaikal Standard Time	(UTC+09:00)	Chita	
Turkey Standard Time	(UTC+03:00)	Istanbul	
Turks And Caicos Standard Time	(UTC-05:00)	Turks and Caicos	
Ulaanbaatar Standard Time	(UTC+08:00)	Ulaanbaatar	This time zone doesn't observe daylight saving time.

Time zone	Standard time offset	Description	Notes
US Eastern Standard Time	(UTC-05:00)	Indiana (East)	
US Mountain Standard Time	(UTC-07:00)	Arizona	This time zone doesn't observe daylight saving time.
UTC	UTC	Coordinated Universal Time	This time zone doesn't observe daylight saving time.
UTC-02	(UTC-02:00)	Coordinated Universal Time-02	This time zone doesn't observe daylight saving time.
UTC-08	(UTC-08:00)	Coordinated Universal Time-08	
UTC-09	(UTC-09:00)	Coordinated Universal Time-09	
UTC-11	(UTC-11:00)	Coordinated Universal Time-11	This time zone doesn't observe daylight saving time.
UTC+12	(UTC+12:00)	Coordinated Universal Time+12	This time zone doesn't observe daylight saving time.
UTC+13	(UTC+13:00)	Coordinated Universal Time+13	
Venezuela Standard Time	(UTC-04:00)	Caracas	This time zone doesn't observe daylight saving time.
Vladivostok Standard Time	(UTC+10:00)	Vladivostok	
Volgograd Standard Time	(UTC+04:00)	Volgograd	
W. Australia Standard Time	(UTC+08:00)	Perth	This time zone doesn't observe daylight saving time.
W. Central Africa Standard Time	(UTC+01:00)	West Central Africa	This time zone doesn't observe daylight saving time.
W. Europe Standard Time	(UTC+01:00)	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	
W. Mongolia Standard Time	(UTC+07:00)	Hovd	
West Asia Standard Time	(UTC+05:00)	Ashgabat, Tashkent	This time zone doesn't observe daylight saving time.

Time zone	Standard time offset	Description	Notes
West Bank Standard Time	(UTC+02:00)	Gaza, Hebron	
West Pacific Standard Time	(UTC+10:00)	Guam, Port Moresby	This time zone doesn't observe daylight saving time.
Yakutsk Standard Time	(UTC+09:00)	Yakutsk	

Licensing Microsoft SQL Server on Amazon RDS

When you set up an Amazon RDS DB instance for Microsoft SQL Server, the software license is included.

This means that you don't need to purchase SQL Server licenses separately. AWS holds the license for the SQL Server database software. Amazon RDS pricing includes the software license, underlying hardware resources, and Amazon RDS management capabilities.

Amazon RDS supports the following Microsoft SQL Server editions:

- Enterprise
- Standard
- Web
- Express

Note

Licensing for SQL Server Web Edition supports only public and internet-accessible webpages, websites, web applications, and web services. This level of support is required for compliance with Microsoft's usage rights. For more information, see [AWS service terms](#).

Amazon RDS supports Multi-AZ deployments for DB instances running Microsoft SQL Server by using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). There are no additional licensing requirements for Multi-AZ deployments. For more information, see [Multi-AZ deployments for Amazon RDS for Microsoft SQL Server \(p. 1129\)](#).

Restoring license-terminated DB instances

Amazon RDS takes snapshots of license-terminated DB instances. If your instance is terminated for licensing issues, you can restore it from the snapshot to a new DB instance. New DB instances have a license included.

For more information, see [Restoring license-terminated DB instances \(p. 1302\)](#).

Development and test

Because of licensing requirements, we can't offer SQL Server Developer Edition on Amazon RDS. You can use Express Edition for many development, testing, and other nonproduction needs. However, if you need the full feature capabilities of an enterprise-level installation of SQL Server for development, you can download and install SQL Server Developer Edition (and other MSDN products) on Amazon EC2. Dedicated infrastructure isn't required for Developer Edition. By using your own host, you also gain access to other programmability features that are not accessible on Amazon RDS. For more information on the difference between SQL Server editions, see [Editions and supported features of SQL Server 2017](#) in the Microsoft documentation.

Connecting to a DB instance running the Microsoft SQL Server database engine

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to the DB instance. In this topic, you connect to your DB instance by using either Microsoft SQL Server Management Studio (SSMS) or SQL Workbench/J.

For an example that walks you through the process of creating and connecting to a sample DB instance, see [Creating a Microsoft SQL Server DB instance and connecting to it \(p. 162\)](#).

Before you connect

Before you can connect to your DB instance, it has to be available and accessible.

1. Make sure that its status is available. You can check this on the details page for your instance in the AWS Management Console or by using the [describe-db-instances](#) AWS CLI command.

The screenshot shows the AWS RDS Details page for a database instance named "database-2".
Summary:

DB identifier database-2	CPU 7.42%	Status Available (highlighted with a red circle)	Class db.r4.large
Role Instance	Current activity 0 Sessions	Engine SQL Server Standard Edition	Region & AZ us-west-2d

Connectivity & security:

Endpoint & port Endpoint: database-2.us-west-2.rds.amazonaws.com Port: 1433	Networking Availability zone: us-west-2d VPC: vpc- Subnet group: default	Security VPC security groups: default (sg- Public accessibility: Yes (highlighted with a red circle) Certificate authority: rds-ca-2019
---	---	--

2. Make sure that it is publicly accessible. You can check this when you check the availability.
3. Make sure that the inbound rules of your VPC security group allow access to your DB instance. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Finding the DB instance endpoint and port number

You need both the endpoint and the port number to connect to the DB instance.

To find the endpoint and port

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the upper-right corner of the Amazon RDS console, choose the AWS Region of your DB instance.
3. Find the Domain Name System (DNS) name (endpoint) and port number for your DB instance:
 - a. Open the RDS console and choose **Databases** to display a list of your DB instances.
 - b. Choose the SQL Server DB instance name to display its details.
 - c. On the **Connectivity & security** tab, copy the endpoint.

The screenshot shows the 'Summary' tab of the RDS console for a database named 'database-2'. The 'Connectivity & security' tab is active. Under 'Endpoint & port', the 'Endpoint' field shows 'database-2. [REDACTED].us-east-2.rds.amazonaws.com' and the 'Port' field shows '1433'.

- d. Note the port number.

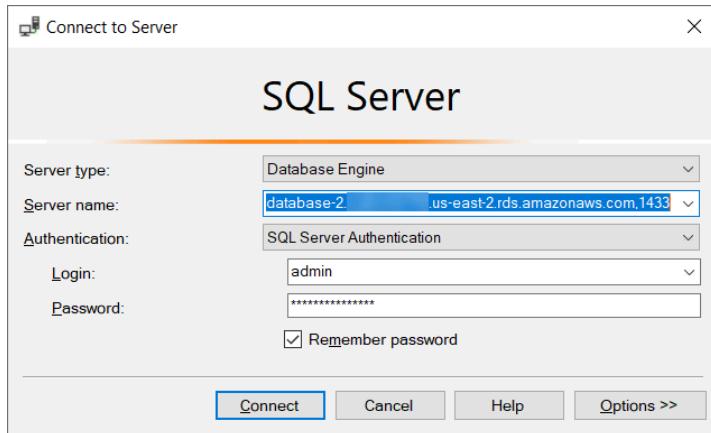
Connecting to your DB instance with Microsoft SQL Server Management Studio

In this procedure, you connect to your sample DB instance by using Microsoft SQL Server Management Studio (SSMS). To download a standalone version of this utility, see [Download SQL Server Management Studio \(SSMS\)](#) in the Microsoft documentation.

To connect to a DB instance using SSMS

1. Start SQL Server Management Studio.

The **Connect to Server** dialog box appears.



2. Provide the information for your DB instance:
 - a. For **Server type**, choose **Database Engine**.
 - b. For **Server name**, enter the DNS name (endpoint) and port number of your DB instance, separated by a comma.

Important

Change the colon between the endpoint and port number to a comma.

Your server name should look like the following example.

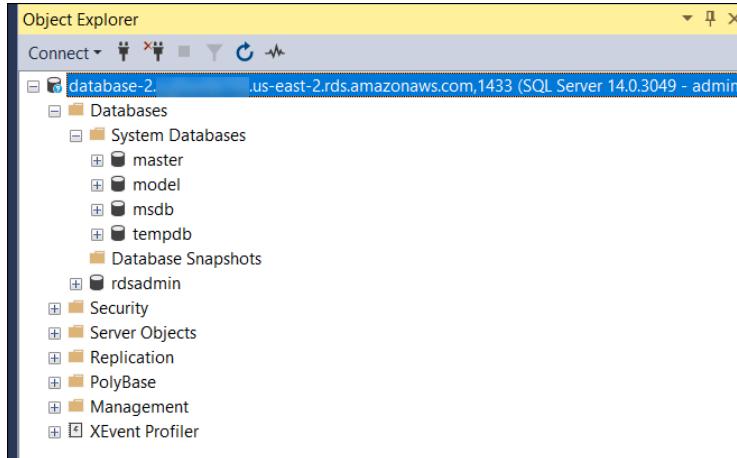
database-2.cg034itsfake.us-east-1.rds.amazonaws.com,1433

- c. For **Authentication**, choose **SQL Server Authentication**.
 - d. For **Login**, enter the master user name for your DB instance.
 - e. For **Password**, enter the password for your DB instance.
3. Choose **Connect**.

After a few moments, SSMS connects to your DB instance.

If you can't connect to your DB instance, see [Security group considerations \(p. 1089\)](#) and [Troubleshooting connections to your SQL Server DB instance \(p. 1089\)](#).

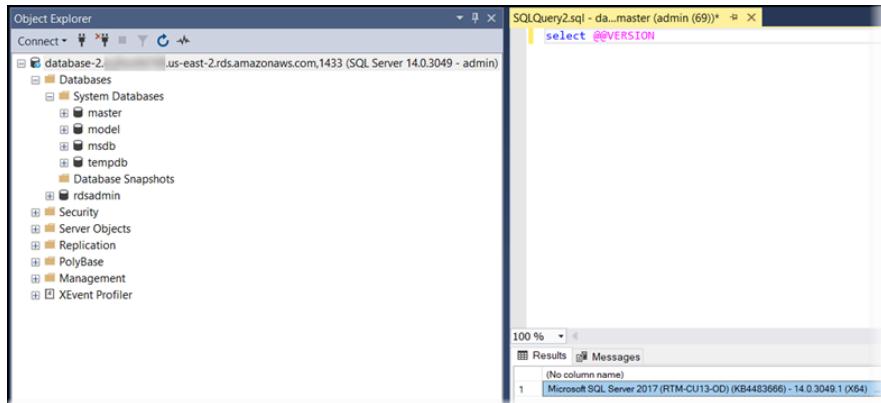
4. Your SQL Server DB instance comes with SQL Server's standard built-in system databases (master, model, msdb, and tempdb). To explore the system databases, do the following:
 - a. In SSMS, on the **View** menu, choose **Object Explorer**.
 - b. Expand your DB instance, expand **Databases**, and then expand **System Databases**.



5. Your SQL Server DB instance also comes with a database named `rdsadmin`. Amazon RDS uses this database to store the objects that it uses to manage your database. The `rdsadmin` database also includes stored procedures that you can run to perform advanced tasks. For more information, see [Common DBA tasks for Microsoft SQL Server \(p. 1291\)](#).
6. You can now start creating your own databases and running queries against your DB instance and databases as usual. To run a test query against your DB instance, do the following:
 - a. In SSMS, on the **File** menu point to **New** and then choose **Query with Current Connection**.
 - b. Enter the following SQL query.

```
select @@VERSION
```

- c. Run the query. SSMS returns the SQL Server version of your Amazon RDS DB instance.



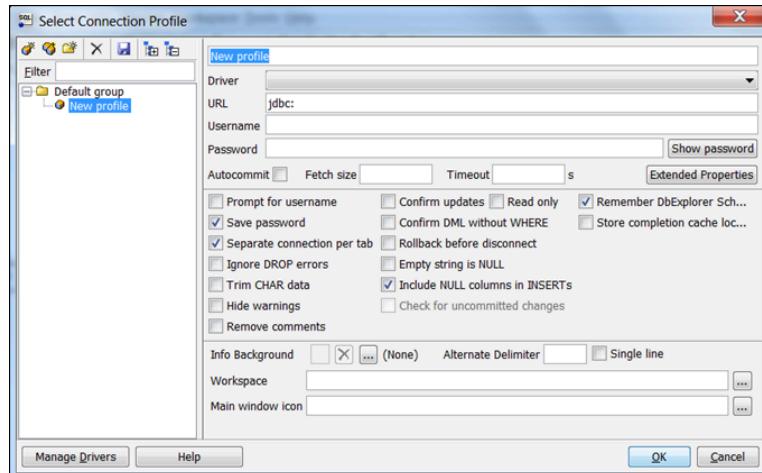
Connecting to your DB instance with SQL Workbench/J

This example shows how to connect to a DB instance running the Microsoft SQL Server database engine by using the SQL Workbench/J database tool. To download SQL Workbench/J, see [SQL Workbench/J](#).

SQL Workbench/J uses JDBC to connect to your DB instance. You also need the JDBC driver for SQL Server. To download this driver, see [Microsoft JDBC drivers 4.1 \(preview\) and 4.0 for SQL Server](#).

To connect to a DB instance using SQL Workbench/J

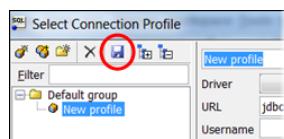
1. Open SQL Workbench/J. The **Select Connection Profile** dialog box appears, as shown following.



2. In the first box at the top of the dialog box, enter a name for the profile.
3. For **Driver**, choose **SQL JDBC 4.0**.
4. For **URL**, enter **jdbc:sqlserver://**, then enter the endpoint of your DB instance. For example, the URL value might be the following.

```
jdbc:sqlserver://sqlsvr-pdz.abcd12340.us-west-2.rds.amazonaws.com:1433
```

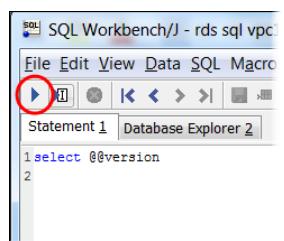
5. For **Username**, enter the master user name for the DB instance.
6. For **Password**, enter the password for the master user.
7. Choose the save icon in the dialog toolbar, as shown following.



8. Choose **OK**. After a few moments, SQL Workbench/J connects to your DB instance. If you can't connect to your DB instance, see [Security group considerations \(p. 1089\)](#) and [Troubleshooting connections to your SQL Server DB instance \(p. 1089\)](#).
9. In the query pane, enter the following SQL query.

```
select @@VERSION
```

10. Choose the Execute icon in the toolbar, as shown following.



The query returns the version information for your DB instance, similar to the following.

Microsoft SQL Server 2017 (RTM-CU22) (KB4577467) - 14.0.3356.20 (X64)

Security group considerations

To connect to your DB instance, your DB instance must be associated with a security group. This security group contains the IP addresses and network configuration that you use to access the DB instance. You might have associated your DB instance with an appropriate security group when you created your DB instance. If you assigned a default, no-configured security group when you created your DB instance, your DB instance firewall prevents connections.

In some cases, you might need to create a new security group to make access possible. For instructions on creating a new security group, see [Controlling access with security groups \(p. 2085\)](#). For a topic that walks you through the process of setting up rules for your VPC security group, see [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).

After you have created the new security group, modify your DB instance to associate it with the security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

You can enhance security by using SSL to encrypt connections to your DB instance. For more information, see [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#).

Troubleshooting connections to your SQL Server DB instance

The following table shows error messages that you might encounter when you attempt to connect to your SQL Server DB instance. For more information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Issue	Troubleshooting suggestions
Could not open a connection to SQL Server – Microsoft SQL Server, Error: 53	<p>Make sure that you specified the server name correctly. For Server name, enter the DNS name and port number of your sample DB instance, separated by a comma.</p> <p>Important If you have a colon between the DNS name and port number, change the colon to a comma. Your server name should look like the following example.</p> <p>sample-instance.cg034itsfake.us-east-1.rds.amazonaws.com,1433</p>
No connection could be made because the target machine actively refused it – Microsoft SQL Server, Error: 10061	You were able to reach the DB instance but the connection was refused. This issue is usually caused by specifying the user name or password incorrectly. Verify the user name and password, then retry.
A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found	The access rules enforced by your local firewall and the IP addresses authorized to access your DB instance might not match. The problem is most likely the inbound rules in your security group.

Issue	Troubleshooting suggestions
or was not accessible... The wait operation timed out – Microsoft SQL Server, Error: 258	Your database instance must be publicly accessible. To connect to it from outside of the VPC, the instance must have a public IP address assigned.

Updating applications to connect to Microsoft SQL Server DB instances using new SSL/TLS certificates

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your RDS DB instances using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.

This topic can help you to determine whether any client applications use SSL/TLS to connect to your DB instances. If they do, you can further check whether those applications require certificate verification to connect.

Note

Some applications are configured to connect to SQL Server DB instances only if they can successfully verify the certificate on the server.

For such applications, you must update your client application trust stores to include the new CA certificates.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB instances. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see [Rotating your SSL/TLS certificate \(p. 2007\)](#). For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For information about using SSL/TLS with Microsoft SQL Server DB instances, see [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#).

Topics

- [Determining whether any applications are connecting to your Microsoft SQL Server DB instance using SSL \(p. 1091\)](#)
- [Determining whether a client requires certificate verification in order to connect \(p. 1092\)](#)
- [Updating your application trust store \(p. 1093\)](#)

Determining whether any applications are connecting to your Microsoft SQL Server DB instance using SSL

Check the DB instance configuration for the value of the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to 0 (off). If the `rds.force_ssl` parameter is set to 1 (on), clients are required to use SSL/TLS for connections. For more information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

Run the following query to get the current encryption option for all the open connections to a DB instance. The column `ENCRYPT_OPTION` returns TRUE if the connection is encrypted.

```
select SESSION_ID,
       ENCRYPT_OPTION,
       NET_TRANSPORT,
       AUTH_SCHEME
  from SYS.DM_EXEC_CONNECTIONS
```

This query shows only the current connections. It doesn't show whether applications that have connected and disconnected in the past have used SSL.

Determining whether a client requires certificate verification in order to connect

You can check whether different types of clients require certificate verification to connect.

Note

If you use connectors other than the ones listed, see the specific connector's documentation for information about how it enforces encrypted connections. For more information, see [Connection modules for Microsoft SQL databases](#) in the Microsoft SQL Server documentation.

SQL Server Management Studio

Check whether encryption is enforced for SQL Server Management Studio connections:

1. Launch SQL Server Management Studio.
2. For **Connect to server**, enter the server information, login user name, and password.
3. Choose **Options**.
4. Check if **Encrypt connection** is selected in the connect page.

For more information about SQL Server Management Studio, see [Use SQL Server Management Studio](#).

Sqlcmd

The following example with the sqlcmd client shows how to check a script's SQL Server connection to determine whether successful connections require a valid certificate. For more information, see [Connecting with sqlcmd](#) in the Microsoft SQL Server documentation.

When using sqlcmd, an SSL connection requires verification against the server certificate if you use the -N command argument to encrypt connections, as in the following example.

```
$ sqlcmd -N -S dbinstance.rds.amazonaws.com -d ExampleDB
```

Note

If sqlcmd is invoked with the -C option, it trusts the server certificate, even if that doesn't match the client-side trust store.

ADO.NET

In the following example, the application connects using SSL, and the server certificate must be verified.

```
using SQLC = Microsoft.Data.SqlClient;  
  
...  
  
static public void Main()  
{  
    using (var connection = new SQLC.SqlConnection(  
        "Server=tcp:dbinstance.rds.amazonaws.com;" +  
        "Database=ExampleDB;User ID=LOGIN_NAME;" +  
        "Password=YOUR_PASSWORD;" +  
        "Encrypt=True;TrustServerCertificate=False;"  
    ))
```

```
{  
    connection.Open();  
    ...  
}
```

Java

In the following example, the application connects using SSL, and the server certificate must be verified.

```
String connectionUrl =  
    "jdbc:sqlserver://dbinstance.rds.amazonaws.com;" +  
    "databaseName=ExampleDB;integratedSecurity=true;" +  
    "encrypt=true;trustServerCertificate=false";
```

To enable SSL encryption for clients that connect using JDBC, you might need to add the Amazon RDS certificate to the Java CA certificate store. For instructions, see [Configuring the client for encryption](#) in the Microsoft SQL Server documentation. You can also provide the trusted CA certificate file name directly by appending `trustStore=path-to-certificate-trust-store-file` to the connection string.

Note

If you use `TrustServerCertificate=true` (or its equivalent) in the connection string, the connection process skips the trust chain validation. In this case, the application connects even if the certificate can't be verified. Using `TrustServerCertificate=false` enforces certificate validation and is a best practice.

Updating your application trust store

You can update the trust store for applications that use Microsoft SQL Server. For instructions, see [Encrypting specific connections \(p. 1136\)](#). Also, see [Configuring the client for encryption](#) in the Microsoft SQL Server documentation.

If you are using an operating system other than Microsoft Windows, see the software distribution documentation for SSL/TLS implementation for information about adding a new root CA certificate. For example, OpenSSL and GnuTLS are popular options. Use the implementation method to add trust to the RDS root CA certificate. Microsoft provides instructions for configuring certificates on some systems.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

When you update the trust store, you can retain older certificates in addition to adding the new certificates.

Upgrading the Microsoft SQL Server DB engine

When Amazon RDS supports a new version of a database engine, you can upgrade your DB instances to the new version. There are two kinds of upgrades for SQL Server DB instances: major version upgrades and minor version upgrades.

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, you must manually perform major version upgrades of your DB instances. You can initiate a major version upgrade by modifying your DB instance. However, before you perform a major version upgrade, we recommend that you test the upgrade by following the steps described in [Testing an upgrade \(p. 1097\)](#).

In contrast, *minor version upgrades* include only changes that are backward-compatible with existing applications. You can initiate a minor version upgrade manually by modifying your DB instance.

Alternatively, you can enable the **Auto minor version upgrade** option when creating or modifying a DB instance. Doing so means that your DB instance is automatically upgraded after Amazon RDS tests and approves the new version. You can confirm whether the minor version upgrade will be automatic by using the `describe-db-engine-versions` AWS CLI command. For example:

```
aws rds describe-db-engine-versions --engine sqlserver-se --engine-version 14.00.3049.1.v1
```

In the following example, the CLI command returns a response indicating that upgrades are automatic.

```
...
"ValidUpgradeTarget": [
    {
        "Engine": "sqlserver-se",
        "EngineVersion": "14.00.3192.2.v1",
        "Description": "SQL Server 2017 14.00.3192.2.v1",
        "AutoUpgrade": true,
        "IsMajorVersionUpgrade": false
    }
]
...
```

For more information about performing upgrades, see [Upgrading a SQL Server DB instance \(p. 1098\)](#). For information about what SQL Server versions are available on Amazon RDS, see [Amazon RDS for Microsoft SQL Server \(p. 1058\)](#).

Topics

- [Overview of upgrading \(p. 1095\)](#)
- [Major version upgrades \(p. 1095\)](#)
- [Multi-AZ and in-memory optimization considerations \(p. 1096\)](#)
- [Option group considerations \(p. 1097\)](#)
- [Parameter group considerations \(p. 1097\)](#)
- [Testing an upgrade \(p. 1097\)](#)
- [Upgrading a SQL Server DB instance \(p. 1098\)](#)
- [Upgrading deprecated DB instances before support ends \(p. 1098\)](#)

Overview of upgrading

Amazon RDS takes two DB snapshots during the upgrade process. The first DB snapshot is of the DB instance before any upgrade changes have been made. The second DB snapshot is taken after the upgrade finishes.

Note

Amazon RDS only takes DB snapshots if you have set the backup retention period for your DB instance to a number greater than 0. To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

After an upgrade is completed, you can't revert to the previous version of the database engine. If you want to return to the previous version, restore from the DB snapshot that was taken before the upgrade to create a new DB instance.

During a minor or major version upgrade of SQL Server, the **Free Storage Space** and **Disk Queue Depth** metrics will display -1. After the upgrade is completed, both metrics will return to normal.

Major version upgrades

Amazon RDS currently supports the following major version upgrades to a Microsoft SQL Server DB instance.

You can upgrade your existing DB instance to SQL Server 2017 or 2019 from any version except SQL Server 2008. To upgrade from SQL Server 2008, first upgrade to one of the other versions.

Current version	Supported upgrade versions
SQL Server 2017	SQL Server 2019
SQL Server 2016	SQL Server 2019 SQL Server 2017
SQL Server 2014	SQL Server 2019 SQL Server 2017 SQL Server 2016
SQL Server 2012 (end of support)	SQL Server 2019 SQL Server 2017 SQL Server 2016 SQL Server 2014
SQL Server 2008 R2 (end of support)	SQL Server 2016 SQL Server 2014 SQL Server 2012

You can use an AWS CLI query, such as the following example, to find the available upgrades for a particular database engine version.

Example

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine sqlserver-se \
--engine-version 14.00.3049.1.v1 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" \
--output table
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine sqlserver-se ^
--engine-version 14.00.3049.1.v1 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
--output table
```

The output shows that you can upgrade version 14.00.3049.1 to the latest SQL Server 2017 or 2019 versions.

```
-----|DescribeDBEngineVersions|
+-----+
|   EngineVersion   |
+-----+
| 14.00.3294.2.v1  |
| 14.00.3356.20.v1 |
| 14.00.3381.3.v1  |
| 15.00.4043.16.v1 |
| 15.00.4073.23.v1 |
+-----+
```

Database compatibility level

You can use Microsoft SQL Server database compatibility levels to adjust some database behaviors to mimic previous versions of SQL Server. For more information, see [Compatibility level](#) in the Microsoft documentation.

When you upgrade your DB instance, all existing databases remain at their original compatibility level. For example, if you upgrade from SQL Server 2014 to SQL Server 2016, all existing databases have a compatibility level of 120. Any new database created after the upgrade have compatibility level 130.

You can change the compatibility level of a database by using the ALTER DATABASE command. For example, to change a database named `customeracct` to be compatible with SQL Server 2014, issue the following command:

```
ALTER DATABASE customeracct SET COMPATIBILITY_LEVEL = 120
```

Multi-AZ and in-memory optimization considerations

Amazon RDS supports Multi-AZ deployments for DB instances running Microsoft SQL Server by using SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). For more information, see [Multi-AZ deployments for Amazon RDS for Microsoft SQL Server \(p. 1129\)](#).

If your DB instance is in a Multi-AZ deployment, both the primary and standby instances are upgraded. Amazon RDS does rolling upgrades. You have an outage only for the duration of a failover.

SQL Server 2014 through 2019 Enterprise Edition support in-memory optimization.

Option group considerations

If your DB instance uses a custom DB option group, in some cases Amazon RDS can't automatically assign your DB instance a new option group. For example, when you upgrade to a new major version, you must specify a new option group. We recommend that you create a new option group, and add the same options to it as your existing custom option group.

For more information, see [Creating an option group \(p. 274\)](#) or [Copying an option group \(p. 276\)](#).

Parameter group considerations

If your DB instance uses a custom DB parameter group:

- Amazon RDS automatically reboots the DB instance after an upgrade.
- In some cases, RDS can't automatically assign a new parameter group to your DB instance.

For example, when you upgrade to a new major version, you must specify a new parameter group. We recommend that you create a new parameter group, and configure the parameters as in your existing custom parameter group.

For more information, see [Creating a DB parameter group \(p. 291\)](#) or [Copying a DB parameter group \(p. 298\)](#).

Testing an upgrade

Before you perform a major version upgrade on your DB instance, you should thoroughly test your database, and all applications that access the database, for compatibility with the new version. We recommend that you use the following procedure.

To test a major version upgrade

1. Review [Upgrade SQL Server](#) in the Microsoft documentation for the new version of the database engine to see if there are compatibility issues that might affect your database or applications.
2. If your DB instance uses a custom option group, create a new option group compatible with the new version you are upgrading to. For more information, see [Option group considerations \(p. 1097\)](#).
3. If your DB instance uses a custom parameter group, create a new parameter group compatible with the new version you are upgrading to. For more information, see [Parameter group considerations \(p. 1097\)](#).
4. Create a DB snapshot of the DB instance to be upgraded. For more information, see [Creating a DB snapshot \(p. 448\)](#).
5. Restore the DB snapshot to create a new test DB instance. For more information, see [Restoring from a DB snapshot \(p. 452\)](#).
6. Modify this new test DB instance to upgrade it to the new version, by using one of the following methods:
 - [Console \(p. 360\)](#)
 - [AWS CLI \(p. 361\)](#)
 - [RDS API \(p. 361\)](#)
7. Evaluate the storage used by the upgraded instance to determine if the upgrade requires additional storage.

8. Run as many of your quality assurance tests against the upgraded DB instance as needed to ensure that your database and application work correctly with the new version. Implement any new tests needed to evaluate the impact of any compatibility issues you identified in step 1. Test all stored procedures and functions. Direct test versions of your applications to the upgraded DB instance.
9. If all tests pass, then perform the upgrade on your production DB instance. We recommend that you do not allow write operations to the DB instance until you confirm that everything is working correctly.

Upgrading a SQL Server DB instance

For information about manually or automatically upgrading a SQL Server DB instance, see the following:

- [Upgrading a DB instance engine version \(p. 360\)](#)
- [Best practices for upgrading SQL Server 2008 R2 to SQL Server 2016 on Amazon RDS for SQL Server](#)

Important

If you have any snapshots that are encrypted using AWS KMS, we recommend that you initiate an upgrade before support ends.

Upgrading deprecated DB instances before support ends

After a major version is deprecated, you can't install it on new DB instances. RDS will try to automatically upgrade all existing DB instances.

If you need to restore a deprecated DB instance, you can do point-in-time recovery (PITR) or restore a snapshot. Doing this gives you temporary access a DB instance that uses the version that is being deprecated. However, after a major version is fully deprecated, these DB instances will also be automatically upgraded to a supported version.

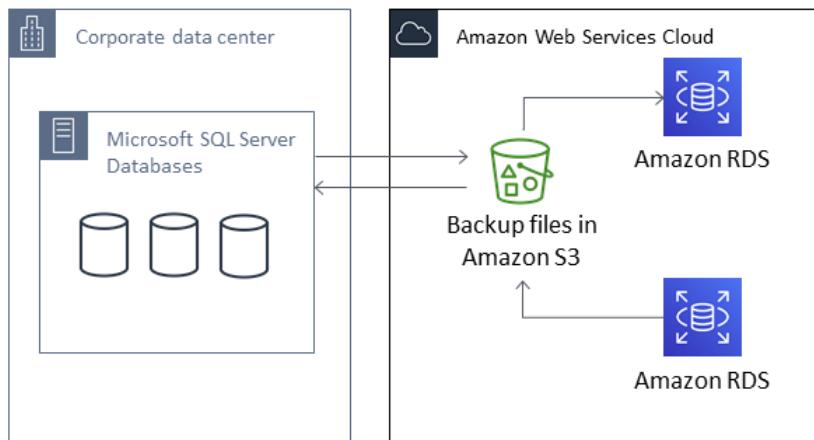
Importing and exporting SQL Server databases using native backup and restore

Amazon RDS supports native backup and restore for Microsoft SQL Server databases using full backup files (.bak files). When you use RDS, you access files stored in Amazon S3 rather than using the local file system on the database server.

For example, you can create a full backup from your local server, store it on S3, and then restore it onto an existing Amazon RDS DB instance. You can also make backups from RDS, store them on S3, and then restore them wherever you want.

Native backup and restore is available in all AWS Regions for Single-AZ and Multi-AZ DB instances, including Multi-AZ DB instances with read replicas. Native backup and restore is available for all editions of Microsoft SQL Server supported on Amazon RDS.

The following diagram shows the supported scenarios.



Using native .bak files to back up and restore databases is usually the fastest way to back up and restore databases. There are many additional advantages to using native backup and restore. For example, you can do the following:

- Migrate databases to or from Amazon RDS.
- Move databases between RDS for SQL Server DB instances.
- Migrate data, schemas, stored procedures, triggers, and other database code inside .bak files.
- Backup and restore single databases, instead of entire DB instances.
- Create copies of databases for development, testing, training, and demonstrations.
- Store and transfer backup files with Amazon S3, for an added layer of protection for disaster recovery.
- Create native backups of databases that have Transparent Data Encryption (TDE) turned on, and restore those backups to on-premises databases. For more information, see [Support for Transparent Data Encryption in SQL Server \(p. 1217\)](#).
- Restore native backups of on-premises databases that have TDE turned on to RDS for SQL Server DB instances. For more information, see [Support for Transparent Data Encryption in SQL Server \(p. 1217\)](#).

Contents

- [Limitations and recommendations \(p. 1100\)](#)
- [Setting up for native backup and restore \(p. 1101\)](#)

- Manually creating an IAM role for native backup and restore (p. 1102)
- Using native backup and restore (p. 1105)
 - Backing up a database (p. 1105)
 - Usage (p. 1105)
 - Examples (p. 1107)
 - Restoring a database (p. 1108)
 - Usage (p. 1108)
 - Examples (p. 1109)
 - Restoring a log (p. 1110)
 - Usage (p. 1110)
 - Examples (p. 1111)
 - Finishing a database restore (p. 1111)
 - Usage (p. 1112)
 - Working with partially restored databases (p. 1112)
 - Dropping a partially restored database (p. 1112)
 - Snapshot restore and point-in-time recovery behavior for partially restored databases (p. 1112)
 - Canceling a task (p. 1112)
 - Usage (p. 1112)
 - Tracking the status of tasks (p. 1112)
 - Usage (p. 1112)
 - Examples (p. 1113)
 - Response (p. 1113)
- Compressing backup files (p. 1115)
- Troubleshooting (p. 1115)
- Importing and exporting SQL Server data using other methods (p. 1117)
 - Importing data into RDS for SQL Server by using a snapshot (p. 1117)
 - Import the data (p. 1120)
 - Generate and Publish Scripts Wizard (p. 1120)
 - Import and Export Wizard (p. 1121)
 - Bulk copy (p. 1121)
 - Exporting data from RDS for SQL Server (p. 1122)
 - SQL Server Import and Export Wizard (p. 1122)
 - SQL Server Generate and Publish Scripts Wizard and bcp utility (p. 1123)

Limitations and recommendations

The following are some limitations to using native backup and restore:

- You can't back up to, or restore from, an Amazon S3 bucket in a different AWS Region from your Amazon RDS DB instance.
- You can't restore a database with the same name as an existing database. Database names are unique.
- We strongly recommend that you don't restore backups from one time zone to a different time zone. If you restore backups from one time zone to a different time zone, you must audit your queries and applications for the effects of the time zone change.
- Amazon S3 has a size limit of 5 TB per file. For native backups of larger databases, you can use multifile backup.

- The maximum database size that can be backed up to S3 depends on the available memory, CPU, I/O, and network resources on the DB instance. The larger the database, the more memory the backup agent consumes. Our testing shows that you can make a compressed backup of a 16-TB database on our newest-generation instance types from 2xlarge instance sizes and larger, given sufficient system resources.
- You can't back up to or restore from more than 10 backup files at the same time.
- A differential backup is based on the last full backup. For differential backups to work, you can't take a snapshot between the last full backup and the differential backup. If you want a differential backup, but a manual or automated snapshot exists, then do another full backup before proceeding with the differential backup.
- Differential and log restores aren't supported for databases with files that have their file_guid (unique identifier) set to NULL.
- You can run up to two backup or restore tasks at the same time.
- You can't perform native log backups from SQL Server on Amazon RDS.
- RDS supports native restores of databases up to 16 TB. Native restores of databases on SQL Server Express Edition are limited to 10 GB.
- You can't do a native backup during the maintenance window, or any time Amazon RDS is in the process of taking a snapshot of the database. If a native backup task overlaps with the RDS daily backup window, the native backup task is canceled.
- On Multi-AZ DB instances, you can only natively restore databases that are backed up in the full recovery model.
- Restoring from differential backups on Multi-AZ instances isn't supported.
- Calling the RDS procedures for native backup and restore within a transaction isn't supported.
- Use a symmetric encryption AWS KMS key to encrypt your backups. Amazon RDS doesn't support asymmetric KMS keys. For more information, see [Creating symmetric encryption KMS keys](#) in the *AWS Key Management Service Developer Guide*.
- Native backup files are encrypted with the specified KMS key using the "Encryption-Only" crypto mode. When you are restoring encrypted backup files, be aware that they were encrypted with the "Encryption-Only" crypto mode.
- You can't restore a database that contains a FILESTREAM file group.

If your database can be offline while the backup file is created, copied, and restored, we recommend that you use native backup and restore to migrate it to RDS. If your on-premises database can't be offline, we recommend that you use the AWS Database Migration Service to migrate your database to Amazon RDS. For more information, see [What is AWS Database Migration Service?](#)

Native backup and restore isn't intended to replace the data recovery capabilities of the cross-region snapshot copy feature. We recommend that you use snapshot copy to copy your database snapshot to another AWS Region for cross-region disaster recovery in Amazon RDS. For more information, see [Copying a DB snapshot \(p. 458\)](#).

Setting up for native backup and restore

To set up for native backup and restore, you need three components:

1. An Amazon S3 bucket to store your backup files.

You must have an S3 bucket to use for your backup files and then upload backups you want to migrate to RDS. If you already have an Amazon S3 bucket, you can use that. If you don't, you can [create a bucket](#). Alternatively, you can choose to have a new bucket created for you when you add the SQLSERVER_BACKUP_RESTORE option by using the AWS Management Console.

For information on using S3, see the *Amazon Simple Storage Service User Guide* for a simple introduction. For more depth, see the *Amazon Simple Storage Service User Guide*.

2. An AWS Identity and Access Management (IAM) role to access the bucket.

If you already have an IAM role, you can use that. You can choose to have a new IAM role created for you when you add the SQLSERVER_BACKUP_RESTORE option by using the AWS Management Console. Alternatively, you can create a new one manually.

If you want to create a new IAM role manually, take the approach discussed in the next section. Do the same if you want to attach trust relationships and permissions policies to an existing IAM role.

3. The SQLSERVER_BACKUP_RESTORE option added to an option group on your DB instance.

To enable native backup and restore on your DB instance, you add the SQLSERVER_BACKUP_RESTORE option to an option group on your DB instance. For more information and instructions, see [Support for native backup and restore in SQL Server \(p. 1214\)](#).

Manually creating an IAM role for native backup and restore

If you want to manually create a new IAM role to use with native backup and restore, you can do so. In this case, you create a role to delegate permissions from the Amazon RDS service to your Amazon S3 bucket. When you create an IAM role, you attach a trust relationship and a permissions policy. The trust relationship allows RDS to assume this role. The permissions policy defines the actions this role can perform. For more information about creating the role, see [Creating a role to delegate permissions to an AWS service](#).

For the native backup and restore feature, use trust relationships and permissions policies similar to the examples in this section. In the following example, we use the service principal name `rds.amazonaws.com` as an alias for all service accounts. In the other examples, we specify an Amazon Resource Name (ARN) to identify another account, user, or role that we're granting access to in the trust policy.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based trust relationships to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the trust relationship, make sure to use the `aws:SourceArn` global condition context key with the full ARN of the resources accessing the role. For native backup and restore, make sure to include both the DB option group and the DB instances, as shown in the following example.

Example trust relationship with global condition context key for native backup and restore

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "rds.amazonaws.com"  
            }  
        }  
    ]  
}
```

```

        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": [
                "aws:SourceArn": [
                    "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier",
                    "arn:aws:rds:Region:my_account_ID:og:option_group_name"
                ]
            ]
        }
    ]
}

```

The following example uses an ARN to specify a resource. For more information on using ARNs, see [Amazon resource names \(ARNs\)](#).

Example permissions policy for native backup and restore without encryption support

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3>ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::bucket_name"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectAttributes",
                "s3:GetObject",
                "s3:PutObject",
                "s3>ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::bucket_name/*"
        }
    ]
}
```

Example permissions policy for native backup and restore with encryption support

If you want to encrypt your backup files, include an encryption key in your permissions policy. For more information about encryption keys, see [Getting started](#) in the *AWS Key Management Service Developer Guide*.

Note

You must use a symmetric encryption KMS key to encrypt your backups. Amazon RDS doesn't support asymmetric KMS keys. For more information, see [Creating symmetric encryption KMS keys](#) in the *AWS Key Management Service Developer Guide*.

The IAM role must also be a key user and key administrator for the KMS key, that is, it must be specified in the key policy. For more information, see [Creating symmetric encryption KMS keys](#) in the *AWS Key Management Service Developer Guide*.

```
{
```

```
"Version": "2012-10-17",
"Statement":
[
    {
        "Effect": "Allow",
        "Action":
            [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Encrypt",
                "kms:Decrypt"
            ],
        "Resource": "arn:aws:kms:region:account-id:key/key-id"
    },
    {
        "Effect": "Allow",
        "Action":
            [
                "s3>ListBucket",
                "s3:GetBucketLocation"
            ],
        "Resource": "arn:aws:s3:::bucket_name"
    },
    {
        "Effect": "Allow",
        "Action":
            [
                "s3:GetObjectAttributes",
                "s3:GetObject",
                "s3:PutObject",
                "s3>ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
        "Resource": "arn:aws:s3:::bucket_name/*"
    }
]
```

Using native backup and restore

After you have enabled and configured native backup and restore, you can start using it. First, you connect to your Microsoft SQL Server database, and then you call an Amazon RDS stored procedure to do the work. For instructions on connecting to your database, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#).

Some of the stored procedures require that you provide an Amazon Resource Name (ARN) to your Amazon S3 bucket and file. The format for your ARN is `arn:aws:s3:::bucket_name/file_name.extension`. Amazon S3 doesn't require an account number or AWS Region in ARNs.

If you also provide an optional KMS key, the format for the ARN of the key is `arn:aws:kms:region:account-id:key/key-id`. For more information, see [Amazon resource names \(ARNs\) and AWS service namespaces](#). You must use a symmetric encryption KMS key to encrypt your backups. Amazon RDS doesn't support asymmetric KMS keys. For more information, see [Creating symmetric encryption KMS keys in the AWS Key Management Service Developer Guide](#).

Note

Whether or not you use a KMS key, the native backup and restore tasks enable server-side Advanced Encryption Standard (AES) 256-bit encryption by default for files uploaded to S3.

For instructions on how to call each stored procedure, see the following topics:

- [Backing up a database \(p. 1105\)](#)
- [Restoring a database \(p. 1108\)](#)
- [Restoring a log \(p. 1110\)](#)
- [Finishing a database restore \(p. 1111\)](#)
- [Working with partially restored databases \(p. 1112\)](#)
- [Canceling a task \(p. 1112\)](#)
- [Tracking the status of tasks \(p. 1112\)](#)

Backing up a database

To back up your database, use the `rds_backup_database` stored procedure.

Note

You can't back up a database during the maintenance window, or while Amazon RDS is taking a snapshot.

Usage

```
exec msdb.dbo.rds_backup_database
@source_db_name='database_name',
@s3_arn_to_backup_to='arn:aws:s3:::bucket_name/file_name.extension',
[@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
[@overwrite_s3_backup_file=0|1],
[@type='DIFFERENTIAL|FULL'],
[@number_of_files=n];
```

The following parameters are required:

- `@source_db_name` – The name of the database to back up.
- `@s3_arn_to_backup_to` – The ARN indicating the Amazon S3 bucket to use for the backup, plus the name of the backup file.

The file can have any extension, but .bak is usually used.

The following parameters are optional:

- @kms_master_key_arn – The ARN for the symmetric encryption KMS key to use to encrypt the item.
 - You can't use the default encryption key. If you use the default key, the database won't be backed up.
 - If you don't specify a KMS key identifier, the backup file won't be encrypted. For more information, see [Encrypting Amazon RDS resources](#).
 - When you specify a KMS key, client-side encryption is used.
 - Amazon RDS doesn't support asymmetric KMS keys. For more information, see [Creating symmetric encryption KMS keys](#) in the *AWS Key Management Service Developer Guide*.
- @overwrite_s3_backup_file – A value that indicates whether to overwrite an existing backup file.
 - 0 – Doesn't overwrite an existing file. This value is the default.

Setting @overwrite_s3_backup_file to 0 returns an error if the file already exists.

- 1 – Overwrites an existing file that has the specified name, even if it isn't a backup file.
- @type – The type of backup.
 - DIFFERENTIAL – Makes a differential backup.
 - FULL – Makes a full backup. This value is the default.

A differential backup is based on the last full backup. For differential backups to work, you can't take a snapshot between the last full backup and the differential backup. If you want a differential backup, but a snapshot exists, then do another full backup before proceeding with the differential backup.

You can look for the last full backup or snapshot using the following example SQL query:

```
select top 1
    database_name
    , backup_start_date
    , backup_finish_date
from msdb.dbo.backupset
where database_name='mydatabase'
and type = 'D'
order by backup_start_date desc;
```

- @number_of_files – The number of files into which the backup will be divided (chunked). The maximum number is 10.
 - Multifile backup is supported for both full and differential backups.
 - If you enter a value of 1 or omit the parameter, a single backup file is created.

Provide the prefix that the files have in common, then suffix that with an asterisk (*). The asterisk can be anywhere in the *file_name* part of the S3 ARN. The asterisk is replaced by a series of alphanumeric strings in the generated files, starting with 1-of-*number_of_files*.

For example, if the file names in the S3 ARN are backup*.bak and you set @number_of_files=4, the backup files generated are backup1-of-4.bak, backup2-of-4.bak, backup3-of-4.bak, and backup4-of-4.bak.

- If any of the file names already exists, and @overwrite_s3_backup_file is 0, an error is returned.
- Multifile backups can only have one asterisk in the *file_name* part of the S3 ARN.
- Single-file backups can have any number of asterisks in the *file_name* part of the S3 ARN. Asterisks aren't removed from the generated file name.

Examples

Example of differential backup

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup1.bak',
@overwrite_s3_backup_file=1,
@type='DIFFERENTIAL';
```

Example of full backup with encryption

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup1.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE',
@overwrite_s3_backup_file=1,
@type='FULL';
```

Example of multifile backup

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@number_of_files=4;
```

Example of multifile differential backup

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@type='DIFFERENTIAL',
@number_of_files=4;
```

Example of multifile backup with encryption

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE',
@number_of_files=4;
```

Example of multifile backup with S3 overwrite

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@overwrite_s3_backup_file=1,
@number_of_files=4;
```

Example of single-file backup with the @number_of_files parameter

This example generates a backup file named backup*.bak.

```
exec msdb.dbo.rds_backup_database
```

```
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@number_of_files=1;
```

Restoring a database

To restore your database, call the `rds_restore_database` stored procedure. Amazon RDS creates an initial snapshot of the database after the restore task is complete and the database is open.

Usage

```
exec msdb.dbo.rds_restore_database
    @restore_db_name='database_name',
    @s3_arn_to_restore_from='arn:aws:s3:::bucket_name/file_name.extension',
    @with_norecovery=0|1,
    [@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
    [@type='DIFFERENTIAL|FULL'];
```

The following parameters are required:

- `@restore_db_name` – The name of the database to restore. Database names are unique. You can't restore a database with the same name as an existing database.
- `@s3_arn_to_restore_from` – The ARN indicating the Amazon S3 prefix and names of the backup files used to restore the database.
 - For a single-file backup, provide the entire file name.
 - For a multifile backup, provide the prefix that the files have in common, then suffix that with an asterisk (*).
 - If `@s3_arn_to_restore_from` is empty, the following error message is returned: S3 ARN prefix cannot be empty.

The following parameter is required for differential restores, but optional for full restores:

- `@with_norecovery` – The recovery clause to use for the restore operation.
 - Set it to 0 to restore with RECOVERY. In this case, the database is online after the restore.
 - Set it to 1 to restore with NORECOVERY. In this case, the database remains in the RESTORING state after restore task completion. With this approach, you can do later differential restores.
 - For DIFFERENTIAL restores, specify 0 or 1.
 - For FULL restores, this value defaults to 0.

The following parameters are optional:

- `@kms_master_key_arn` – If you encrypted the backup file, the KMS key to use to decrypt the file.
When you specify a KMS key, client-side encryption is used.
- `@type` – The type of restore. Valid types are DIFFERENTIAL and FULL. The default value is FULL.

Note

For differential restores, either the database must be in the RESTORING state or a task must already exist that restores with NORECOVERY.

You can't restore later differential backups while the database is online.

You can't submit a restore task for a database that already has a pending restore task with RECOVERY.

Full restores with NORECOVERY and differential restores aren't supported on Multi-AZ instances.

Restoring a database on a Multi-AZ instance with read replicas is similar to restoring a database on a Multi-AZ instance. You don't have to take any additional actions to restore a database on a replica.

Examples

Example of single-file restore

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak';
```

Example of multifile restore

To avoid errors when restoring multiple files, make sure that all the backup files have the same prefix, and that no other files use that prefix.

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup*';
```

Example of full database restore with RECOVERY

The following three examples perform the same task, full restore with RECOVERY.

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak';
```

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
[@type='DIFFERENTIAL | FULL'];
```

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='FULL',
@with_norecovery=0;
```

Example of full database restore with encryption

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Example of full database restore with NORECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='FULL',
@with_norecovery=1;
```

Example of differential restore with NORECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='DIFFERENTIAL',
@with_norecovery=1;
```

Example of differential restore with RECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='DIFFERENTIAL',
@with_norecovery=0;
```

Restoring a log

To restore your log, call the `rds_restore_log` stored procedure.

Usage

```
exec msdb.dbo.rds_restore_log
@restore_db_name='database_name',
@s3_arn_to_restore_from='arn:aws:s3:::bucket_name/log_file_name.extension',
[@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
[@with_norecovery=0/1],
[@stopat='datetime'];
```

The following parameters are required:

- `@restore_db_name` – The name of the database whose log to restore.
- `@s3_arn_to_restore_from` – The ARN indicating the Amazon S3 prefix and name of the log file used to restore the log. The file can have any extension, but `.trn` is usually used.

If `@s3_arn_to_restore_from` is empty, the following error message is returned: S3 ARN prefix cannot be empty.

The following parameters are optional:

- `@kms_master_key_arn` – If you encrypted the log, the KMS key to use to decrypt the log.
- `@with_norecovery` – The recovery clause to use for the restore operation. This value defaults to 1.
 - Set it to 0 to restore with RECOVERY. In this case, the database is online after the restore. You can't restore further log backups while the database is online.
 - Set it to 1 to restore with NORECOVERY. In this case, the database remains in the RESTORING state after restore task completion. With this approach, you can do later log restores.
- `@stopat` – A value that specifies that the database is restored to its state at the date and time specified (in datetime format). Only transaction log records written before the specified date and time are applied to the database.

If this parameter isn't specified (it is NULL), the complete log is restored.

Note

For log restores, either the database must be in a state of restoring or a task must already exist that restores with NORECOVERY.

You can't restore log backups while the database is online.
You can't submit a log restore task on a database that already has a pending restore task with RECOVERY.
Log restores aren't supported on Multi-AZ instances.

Examples

Example of log restore

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn';
```

Example of log restore with encryption

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Example of log restore with NORECOVERY

The following two examples perform the same task, log restore with NORECOVERY.

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=1;
```

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn';
```

Example of log restore with RECOVERY

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=0;
```

Example of log restore with STOPAT clause

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=0,
@stopat='2019-12-01 03:57:09';
```

Finishing a database restore

If the last restore task on the database was performed using @with_norecovery=1, the database is now in the RESTORING state. Open this database for normal operation by using the rds_finish_restore stored procedure.

Usage

```
exec msdb.dbo.rds_finish_restore @db_name='database_name';
```

Note

To use this approach, the database must be in the RESTORING state without any pending restore tasks.

The `rds_finish_restore` procedure isn't supported on Multi-AZ instances.

To finish restoring the database, use the master login. Or use the user login that most recently restored the database or log with NORECOVERY.

Working with partially restored databases

Dropping a partially restored database

To drop a partially restored database (left in the RESTORING state), use the `rds_drop_database` stored procedure.

```
exec msdb.dbo.rds_drop_database @db_name='database_name';
```

Note

You can't submit a DROP database request for a database that already has a pending restore or finish restore task.

To drop the database, use the master login. Or use the user login that most recently restored the database or log with NORECOVERY.

Snapshot restore and point-in-time recovery behavior for partially restored databases

Partially restored databases in the source instance (left in the RESTORING state) are dropped from the target instance during snapshot restore and point-in-time recovery.

Canceling a task

To cancel a backup or restore task, call the `rds_cancel_task` stored procedure.

Note

You can't cancel a FINISH_RESTORE task.

Usage

```
exec msdb.dbo.rds_cancel_task @task_id=ID_number;
```

The following parameter is required:

- `@task_id` – The ID of the task to cancel. You can get the task ID by calling `rds_task_status`.

Tracking the status of tasks

To track the status of your backup and restore tasks, call the `rds_task_status` stored procedure. If you don't provide any parameters, the stored procedure returns the status of all tasks. The status for tasks is updated approximately every two minutes. Task history is retained for 36 days.

Usage

```
exec msdb.dbo.rds_task_status
```

```
[@edb_name='database_name'],  
[@task_id=ID_number];
```

The following parameters are optional:

- @db_name – The name of the database to show the task status for.
- @task_id – The ID of the task to show the task status for.

Examples

Example of listing the status for a specific task

```
exec msdb.dbo.rds_task_status @task_id=5;
```

Example of listing the status for a specific database and task

```
exec msdb.dbo.rds_task_status  
@edb_name='my_database',  
@task_id=5;
```

Example of listing all tasks and their statuses on a specific database

```
exec msdb.dbo.rds_task_status @db_name='my_database';
```

Example of listing all tasks and their statuses on the current instance

```
exec msdb.dbo.rds_task_status;
```

Response

The rds_task_status stored procedure returns the following columns.

Column	Description
task_id	The ID of the task.
task_type	Task type depending on the input parameters, as follows: <ul style="list-style-type: none">• For backup tasks:<ul style="list-style-type: none">• BACKUP_DB – Full database backup• BACKUP_DB_DIFFERENTIAL – Differential database backup• For restore tasks:<ul style="list-style-type: none">• RESTORE_DB – Full database restore with RECOVERY• RESTORE_DB_NORECOVERY – Full database restore with NORECOVERY• RESTORE_DB_DIFFERENTIAL – Differential database restore with RECOVERY• RESTORE_DB_DIFFERENTIAL_NORECOVERY – Differential database restore with NORECOVERY• RESTORE_DB_LOG – Log restore with RECOVERY• RESTORE_DB_LOG_NORECOVERY – Log restore with NORECOVERY• For tasks that finish a restore:<ul style="list-style-type: none">• FINISH_RESTORE – Finish restore and open database

Column	Description
	<p>Amazon RDS creates an initial snapshot of the database after it is open on completion of the following restore tasks:</p> <ul style="list-style-type: none"> • RESTORE_DB • RESTORE_DB_DIFFERENTIAL • RESTORE_DB_LOG • FINISH_RESTORE
database_name	The name of the database that the task is associated with.
% complete	The progress of the task as a percent value.
duration (mins)	The amount of time spent on the task, in minutes.
lifecycle	<p>The status of the task. The possible statuses are the following:</p> <ul style="list-style-type: none"> • CREATED – As soon as you call <code>rds_backup_database</code> or <code>rds_restore_database</code>, a task is created and the status is set to CREATED. • IN_PROGRESS – After a backup or restore task starts, the status is set to IN_PROGRESS. It can take up to 5 minutes for the status to change from CREATED to IN_PROGRESS. • SUCCESS – After a backup or restore task completes, the status is set to SUCCESS. • ERROR – If a backup or restore task fails, the status is set to ERROR. For more information about the error, see the <code>task_info</code> column. • CANCEL_REQUESTED – As soon as you call <code>rds_cancel_task</code>, the status of the task is set to CANCEL_REQUESTED. • CANCELLED – After a task is successfully canceled, the status of the task is set to CANCELLED.
task_info	<p>Additional information about the task.</p> <p>If an error occurs while backing up or restoring a database, this column contains information about the error. For a list of possible errors, and mitigation strategies, see Troubleshooting (p. 1115).</p>
last_updated	The date and time that the task status was last updated. The status is updated after every 5 percent of progress.
created_at	The date and time that the task was created.
S3_object_arn	The ARN indicating the Amazon S3 prefix and the name of the file that is being backed up or restored.
overwrite_s3_backup_file	The value of the <code>@overwrite_s3_backup_file</code> parameter specified when calling a backup task. For more information, see Backing up a database (p. 1105) .
KMS_master_key_arn	The ARN for the KMS key used for encryption (for backup) and decryption (for restore).
filepath	Not applicable to native backup and restore tasks.
overwrite_file	Not applicable to native backup and restore tasks.

Compressing backup files

To save space in your Amazon S3 bucket, you can compress your backup files. For more information about compressing backup files, see [Backup compression](#) in the Microsoft documentation.

Compressing your backup files is supported for the following database editions:

- Microsoft SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition

To turn on compression for your backup files, run the following code:

```
exec rdsadmin..rds_set_configuration 'S3 backup compression', 'true';
```

To turn off compression for your backup files, run the following code:

```
exec rdsadmin..rds_set_configuration 'S3 backup compression', 'false';
```

Troubleshooting

The following are issues you might encounter when you use native backup and restore.

Issue	Troubleshooting suggestions
Database backup/restore option is not enabled yet or is in the process of being enabled. Please try again later.	Make sure that you have added the SQLSERVER_BACKUP_RESTORE option to the DB option group associated with your DB instance. For more information, see Adding the native backup and restore option (p. 1214) .
Access Denied	The backup or restore process can't access the backup file. This is usually caused by issues like the following: <ul style="list-style-type: none">• Referencing the incorrect bucket. Referencing the bucket using an incorrect format. Referencing a file name without using the ARN.• Incorrect permissions on the bucket file. For example, if it is created by a different account that is trying to access it now, add the correct permissions.• An IAM policy that is incorrect or incomplete. Your IAM role must include all the necessary elements, including, for example, the correct version. These are highlighted in Importing and exporting SQL Server databases using native backup and restore (p. 1099).
BACKUP DATABASE WITH COMPRESSION isn't supported on <edition_name> Edition	Compressing your backup files is only supported for Microsoft SQL Server Enterprise Edition and Standard Edition. For more information, see Compressing backup files (p. 1115) .
Key <ARN> does not exist	You attempted to restore an encrypted backup, but didn't provide a valid encryption key. Check your encryption key and retry. For more information, see Restoring a database (p. 1108) .

Issue	Troubleshooting suggestions
Please reissue task with correct type and overwrite property	<p>If you attempt to back up your database and provide the name of a file that already exists, but set the overwrite property to false, the save operation fails. To fix this error, either provide the name of a file that doesn't already exist, or set the overwrite property to true.</p> <p>For more information, see Backing up a database (p. 1105).</p> <p>It's also possible that you intended to restore your database, but called the <code>rds_backup_database</code> stored procedure accidentally. In that case, call the <code>rds_restore_database</code> stored procedure instead.</p> <p>For more information, see Restoring a database (p. 1108).</p> <p>If you intended to restore your database and called the <code>rds_restore_database</code> stored procedure, make sure that you provided the name of a valid backup file.</p> <p>For more information, see Using native backup and restore (p. 1105).</p>
Please specify a bucket that is in the same region as RDS instance	<p>You can't back up to, or restore from, an Amazon S3 bucket in a different AWS Region from your Amazon RDS DB instance. You can use Amazon S3 replication to copy the backup file to the correct AWS Region.</p> <p>For more information, see Cross-Region replication in the Amazon S3 documentation.</p>
The specified bucket does not exist	<p>Verify that you have provided the correct ARN for your bucket and file, in the correct format.</p> <p>For more information, see Using native backup and restore (p. 1105).</p>
User <ARN> is not authorized to perform <kms action> on resource <ARN>	<p>You requested an encrypted operation, but didn't provide correct AWS KMS permissions. Verify that you have the correct permissions, or add them.</p> <p>For more information, see Setting up for native backup and restore (p. 1101).</p>
The Restore task is unable to restore from more than 10 backup file(s). Please reduce the number of files matched and try again.	<p>Reduce the number of files that you're trying to restore from. You can make each individual file larger if necessary.</p>
Database ' <i>database_name</i> ' already exists. Two databases that differ only by case or accent are not allowed. Choose a different database name.	<p>You can't restore a database with the same name as an existing database. Database names are unique.</p>

Importing and exporting SQL Server data using other methods

Following, you can find information about using snapshots to import your Microsoft SQL Server data to Amazon RDS. You can also find information about using snapshots to export your data from an RDS DB instance running SQL Server.

If your scenario supports it, it's easier to move data in and out of Amazon RDS by using the native backup and restore functionality. For more information, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Note

Amazon RDS for Microsoft SQL Server doesn't support importing data into the msdb database.

Importing data into RDS for SQL Server by using a snapshot

To import data into a SQL Server DB instance by using a snapshot

1. Create a DB instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
2. Stop applications from accessing the destination DB instance.

If you prevent access to your DB instance while you are importing data, data transfer is faster. Additionally, you don't need to worry about conflicts while data is being loaded if other applications cannot write to the DB instance at the same time. If something goes wrong and you have to roll back to an earlier database snapshot, the only changes that you lose are the imported data. You can import this data again after you resolve the issue.

For information about controlling access to your DB instance, see [Controlling access with security groups \(p. 2085\)](#).

3. Create a snapshot of the target database.

If the target database is already populated with data, we recommend that you take a snapshot of the database before you import the data. If something goes wrong with the data import or you want to discard the changes, you can restore the database to its previous state by using the snapshot. For information about database snapshots, see [Creating a DB snapshot \(p. 448\)](#).

Note

When you take a database snapshot, I/O operations to the database are suspended for a moment (milliseconds) while the backup is in progress.

4. Disable automated backups on the target database.

Disabling automated backups on the target DB instance improves performance while you are importing your data because Amazon RDS doesn't log transactions when automatic backups are disabled. However, there are some things to consider. Automated backups are required to perform a point-in-time recovery. Thus, you can't restore the database to a specific point in time while you are importing data. Additionally, any automated backups that were created on the DB instance are erased unless you choose to retain them.

Choosing to retain the automated backups can help protect you against accidental deletion of data. Amazon RDS also saves the database instance properties along with each automated backup to make it easy to recover. Using this option lets you can restore a deleted database instance to a specified point in time within the backup retention period even after deleting it. Automated backups are automatically deleted at the end of the specified backup window, just as they are for an active database instance.

You can also use previous snapshots to recover the database, and any snapshots that you have taken remain available. For information about automated backups, see [Working with backups \(p. 427\)](#).

5. Disable foreign key constraints, if applicable.

If you need to disable foreign key constraints, you can do so with the following script.

```
--Disable foreign keys on all tables
DECLARE @table_name SYSNAME;
DECLARE @cmd NVARCHAR(MAX);
DECLARE table_cursor CURSOR FOR SELECT name FROM sys.tables;

OPEN table_cursor;
FETCH NEXT FROM table_cursor INTO @table_name;

WHILE @@FETCH_STATUS = 0 BEGIN
    SELECT @cmd = 'ALTER TABLE '+QUOTENAME(@table_name)+' NOCHECK CONSTRAINT ALL';
    EXEC (@cmd);
    FETCH NEXT FROM table_cursor INTO @table_name;
END

CLOSE table_cursor;
DEALLOCATE table_cursor;

GO
```

6. Drop indexes, if applicable.

7. Disable triggers, if applicable.

If you need to disable triggers, you can do so with the following script.

```
--Disable triggers on all tables
DECLARE @enable BIT = 0;
DECLARE @trigger SYSNAME;
DECLARE @table SYSNAME;
DECLARE @cmd NVARCHAR(MAX);
DECLARE trigger_cursor CURSOR FOR SELECT trigger_object.name trigger_name,
    table_object.name table_name
    FROM sysobjects trigger_object
    JOIN sysobjects table_object ON trigger_object.parent_obj = table_object.id
    WHERE trigger_object.type = 'TR';

OPEN trigger_cursor;
FETCH NEXT FROM trigger_cursor INTO @trigger, @table;

WHILE @@FETCH_STATUS = 0 BEGIN
    IF @enable = 1
        SET @cmd = 'ENABLE ';
    ELSE
        SET @cmd = 'DISABLE ';

    SET @cmd = @cmd + ' TRIGGER dbo.'+QUOTENAME(@trigger)+'' ON
    dbo.'+QUOTENAME(@table)+'' ;
    EXEC (@cmd);
    FETCH NEXT FROM trigger_cursor INTO @trigger, @table;
END

CLOSE trigger_cursor;
DEALLOCATE trigger_cursor;

GO
```

8. Query the source SQL Server instance for any logins that you want to import to the destination DB instance.

SQL Server stores logins and passwords in the master database. Because Amazon RDS doesn't grant access to the master database, you cannot directly import logins and passwords into your destination DB instance. Instead, you must query the master database on the source SQL Server instance to generate a data definition language (DDL) file. This file should include all logins and passwords that you want to add to the destination DB instance. This file also should include role memberships and permissions that you want to transfer.

For information about querying the master database, see [How to transfer the logins and the passwords between instances of SQL Server 2005 and SQL Server 2008](#) in the Microsoft Knowledge Base.

The output of the script is another script that you can run on the destination DB instance. The script in the Knowledge Base article has the following code:

```
p.type IN
```

Every place p.type appears, use the following code instead:

```
p.type = 'S'
```

9. Import the data using the method in [Import the data \(p. 1120\)](#).
10. Grant applications access to the target DB instance.

When your data import is complete, you can grant access to the DB instance to those applications that you blocked during the import. For information about controlling access to your DB instance, see [Controlling access with security groups \(p. 2085\)](#).

11. Enable automated backups on the target DB instance.

For information about automated backups, see [Working with backups \(p. 427\)](#).

12. Enable foreign key constraints.

If you disabled foreign key constraints earlier, you can now enable them with the following script.

```
--Enable foreign keys on all tables
DECLARE @table_name SYSNAME;
DECLARE @cmd NVARCHAR(MAX);
DECLARE table_cursor CURSOR FOR SELECT name FROM sys.tables;

OPEN table_cursor;
FETCH NEXT FROM table_cursor INTO @table_name;

WHILE @@FETCH_STATUS = 0 BEGIN
    SELECT @cmd = 'ALTER TABLE '+QUOTENAME(@table_name)+' CHECK CONSTRAINT ALL';
    EXEC (@cmd);
    FETCH NEXT FROM table_cursor INTO @table_name;
END

CLOSE table_cursor;
DEALLOCATE table_cursor;
```

13. Enable indexes, if applicable.
14. Enable triggers, if applicable.

If you disabled triggers earlier, you can now enable them with the following script.

```
--Enable triggers on all tables
DECLARE @enable BIT = 1;
```

```
DECLARE @trigger SYSNAME;
DECLARE @table SYSNAME;
DECLARE @cmd NVARCHAR(MAX);
DECLARE trigger_cursor CURSOR FOR SELECT trigger_object.name trigger_name,
    table_object.name table_name
    FROM sysobjects trigger_object
    JOIN sysobjects table_object ON trigger_object.parent_obj = table_object.id
    WHERE trigger_object.type = 'TR';

OPEN trigger_cursor;
FETCH NEXT FROM trigger_cursor INTO @trigger, @table;

WHILE @@FETCH_STATUS = 0 BEGIN
    IF @enable = 1
        SET @cmd = 'ENABLE ';
    ELSE
        SET @cmd = 'DISABLE ';

    SET @cmd = @cmd + ' TRIGGER dbo.'+QUOTENAME(@trigger)+'' ON
    dbo.'+QUOTENAME(@table)+'' ;
    EXEC (@cmd);
    FETCH NEXT FROM trigger_cursor INTO @trigger, @table;
END

CLOSE trigger_cursor;
DEALLOCATE trigger_cursor;
```

Import the data

Microsoft SQL Server Management Studio is a graphical SQL Server client that is included in all Microsoft SQL Server editions except the Express Edition. SQL Server Management Studio Express is available from Microsoft as a free download. To find this download, see [the Microsoft website](#).

Note

SQL Server Management Studio is available only as a Windows-based application.

SQL Server Management Studio includes the following tools, which are useful in importing data to a SQL Server DB instance:

- Generate and Publish Scripts Wizard
- Import and Export Wizard
- Bulk copy

Generate and Publish Scripts Wizard

The Generate and Publish Scripts Wizard creates a script that contains the schema of a database, the data itself, or both. You can generate a script for a database in your local SQL Server deployment. You can then run the script to transfer the information that it contains to an Amazon RDS DB instance.

Note

For databases of 1 GiB or larger, it's more efficient to script only the database schema. You then use the Import and Export Wizard or the bulk copy feature of SQL Server to transfer the data.

For detailed information about the Generate and Publish Scripts Wizard, see the [Microsoft SQL Server documentation](#).

In the wizard, pay particular attention to the advanced options on the **Set Scripting Options** page to ensure that everything you want your script to include is selected. For example, by default, database triggers are not included in the script.

When the script is generated and saved, you can use SQL Server Management Studio to connect to your DB instance and then run the script.

Import and Export Wizard

The Import and Export Wizard creates a special Integration Services package, which you can use to copy data from your local SQL Server database to the destination DB instance. The wizard can filter which tables and even which tuples within a table are copied to the destination DB instance.

Note

The Import and Export Wizard works well for large datasets, but it might not be the fastest way to remotely export data from your local deployment. For an even faster way, consider the SQL Server bulk copy feature.

For detailed information about the Import and Export Wizard, see the [Microsoft SQL Server documentation](#).

In the wizard, on the **Choose a Destination** page, do the following:

- For **Server Name**, type the name of the endpoint for your DB instance.
- For the server authentication mode, choose **Use SQL Server Authentication**.
- For **User name** and **Password**, type the credentials for the master user that you created for the DB instance.

Bulk copy

The SQL Server bulk copy feature is an efficient means of copying data from a source database to your DB instance. Bulk copy writes the data that you specify to a data file, such as an ASCII file. You can then run bulk copy again to write the contents of the file to the destination DB instance.

This section uses the **bcp** utility, which is included with all editions of SQL Server. For detailed information about bulk import and export operations, see [the Microsoft SQL Server documentation](#).

Note

Before you use bulk copy, you must first import your database schema to the destination DB instance. The Generate and Publish Scripts Wizard, described earlier in this topic, is an excellent tool for this purpose.

The following command connects to the local SQL Server instance. It generates a tab-delimited file of a specified table in the C:\ root directory of your existing SQL Server deployment. The table is specified by its fully qualified name, and the text file has the same name as the table that is being copied.

```
bcp dbname.schema_name.table_name out C:\table_name.txt -n -S localhost -U username -P password -b 10000
```

The preceding code includes the following options:

- -n specifies that the bulk copy uses the native data types of the data to be copied.
- -S specifies the SQL Server instance that the *bcp* utility connects to.
- -U specifies the user name of the account to log in to the SQL Server instance.
- -P specifies the password for the user specified by -U.
- -b specifies the number of rows per batch of imported data.

Note

There might be other parameters that are important to your import situation. For example, you might need the -E parameter that pertains to identity values. For more information; see

the full description of the command line syntax for the **bcp** utility in the [Microsoft SQL Server documentation](#).

For example, suppose that a database named `store` that uses the default schema, `dbo`, contains a table named `customers`. The user account `admin`, with the password `insecure`, copies 10,000 rows of the `customers` table to a file named `customers.txt`.

```
bcp store.dbo.customers out C:\customers.txt -n -S localhost -U admin -P insecure -b 10000
```

After you generate the data file, you can upload the data to your DB instance by using a similar command. Beforehand, create the database and schema on the target DB instance. Then use the `in` argument to specify an input file instead of `out` to specify an output file. Instead of using `localhost` to specify the local SQL Server instance, specify the endpoint of your DB instance. If you use a port other than 1433, specify that too. The user name and password are the master user and password for your DB instance. The syntax is as follows.

```
bcp dbname.schema_name.table_name in C:\table_name.txt -n -S endpoint,port -  
U master_user_name -P master_user_password -b 10000
```

To continue the previous example, suppose that the master user name is `admin`, and the password is `insecure`. The endpoint for the DB instance is `rds.ckz2kqd4qsn1.us-east-1.rds.amazonaws.com`, and you use port 4080. The command is as follows.

```
bcp store.dbo.customers in C:\customers.txt -n -S rds.ckz2kqd4qsn1.us-east-1.rds.amazonaws.com,4080 -U admin -P insecure -b 10000
```

Exporting data from RDS for SQL Server

You can choose one of the following options to export data from an RDS for SQL Server DB instance:

- **Native database backup using a full backup file (.bak)** – Using .bak files to backup databases is heavily optimized, and is usually the fastest way to export data. For more information, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).
- **SQL Server Import and Export Wizard** – For more information, see [SQL Server Import and Export Wizard \(p. 1122\)](#).
- **SQL Server Generate and Publish Scripts Wizard and bcp utility** – For more information, see [SQL Server Generate and Publish Scripts Wizard and bcp utility \(p. 1123\)](#).

SQL Server Import and Export Wizard

You can use the SQL Server Import and Export Wizard to copy one or more tables, views, or queries from your RDS for SQL Server DB instance to another data store. This choice is best if the target data store is not SQL Server. For more information, see [SQL Server Import and Export Wizard](#) in the SQL Server documentation.

The SQL Server Import and Export Wizard is available as part of Microsoft SQL Server Management Studio. This graphical SQL Server client is included in all Microsoft SQL Server editions except the Express Edition. SQL Server Management Studio is available only as a Windows-based application. SQL Server Management Studio Express is available from Microsoft as a free download. To find this download, see [the Microsoft website](#).

To use the SQL Server Import and Export Wizard to export data

1. In SQL Server Management Studio, connect to your RDS for SQL Server DB instance. For details on how to do this, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#).

2. In **Object Explorer**, expand **Databases**, open the context (right-click) menu for the source database, choose **Tasks**, and then choose **Export Data**. The wizard appears.
 3. On the **Choose a Data Source** page, do the following:
 - a. For **Data source**, choose **SQL Server Native Client 11.0**.
 - b. Verify that the **Server name** box shows the endpoint of your RDS for SQL Server DB instance.
 - c. Select **Use SQL Server Authentication**. For **User name** and **Password**, type the master user name and password of your DB instance.
 - d. Verify that the **Database** box shows the database from which you want to export data.
 - e. Choose **Next**.
 4. On the **Choose a Destination** page, do the following:
 - a. For **Destination**, choose **SQL Server Native Client 11.0**.
- Note**
Other target data sources are available. These include .NET Framework data providers, OLE DB providers, SQL Server Native Client providers, ADO.NET providers, Microsoft Office Excel, Microsoft Office Access, and the Flat File source. If you choose to target one of these data sources, skip the remainder of step 4. For details on the connection information to provide next, see [Choose a destination](#) in the SQL Server documentation.
- b. For **Server name**, type the server name of the target SQL Server DB instance.
 - c. Choose the appropriate authentication type. Type a user name and password if necessary.
 - d. For **Database**, choose the name of the target database, or choose **New** to create a new database to contain the exported data.
- If you choose **New**, see [Create database](#) in the SQL Server documentation for details on the database information to provide.
- e. Choose **Next**.
 5. On the **Table Copy or Query** page, choose **Copy data from one or more tables or views** or **Write a query to specify the data to transfer**. Choose **Next**.
 6. If you chose **Write a query to specify the data to transfer**, you see the **Provide a Source Query** page. Type or paste in a SQL query, and then choose **Parse** to verify it. Once the query validates, choose **Next**.
 7. On the **Select Source Tables and Views** page, do the following:
 - a. Select the tables and views that you want to export, or verify that the query you provided is selected.
 - b. Choose **Edit Mappings** and specify database and column mapping information. For more information, see [Column mappings](#) in the SQL Server documentation.
 - c. (Optional) To see a preview of data to be exported, select the table, view, or query, and then choose **Preview**.
 - d. Choose **Next**.
 8. On the **Run Package** page, verify that **Run immediately** is selected. Choose **Next**.
 9. On the **Complete the Wizard** page, verify that the data export details are as you expect. Choose **Finish**.
 10. On the **The execution was successful** page, choose **Close**.

SQL Server Generate and Publish Scripts Wizard and bcp utility

You can use the SQL Server Generate and Publish Scripts Wizard to create scripts for an entire database or just selected objects. You can run these scripts on a target SQL Server DB instance to recreate the

scripted objects. You can then use the bcp utility to bulk export the data for the selected objects to the target DB instance. This choice is best if you want to move a whole database (including objects other than tables) or large quantities of data between two SQL Server DB instances. For a full description of the bcp command-line syntax, see [bcp utility](#) in the Microsoft SQL Server documentation.

The SQL Server Generate and Publish Scripts Wizard is available as part of Microsoft SQL Server Management Studio. This graphical SQL Server client is included in all Microsoft SQL Server editions except the Express Edition. SQL Server Management Studio is available only as a Windows-based application. SQL Server Management Studio Express is available from Microsoft as a [free download](#).

To use the SQL Server Generate and Publish Scripts Wizard and the bcp utility to export data

1. In SQL Server Management Studio, connect to your RDS for SQL Server DB instance. For details on how to do this, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#).
2. In **Object Explorer**, expand the **Databases** node and select the database you want to script.
3. Follow the instructions in [Generate and publish scripts Wizard](#) in the SQL Server documentation to create a script file.
4. In SQL Server Management Studio, connect to your target SQL Server DB instance.
5. With the target SQL Server DB instance selected in **Object Explorer**, choose **Open** on the **File** menu, choose **File**, and then open the script file.
6. If you have scripted the entire database, review the CREATE DATABASE statement in the script. Make sure that the database is being created in the location and with the parameters that you want. For more information, see [CREATE DATABASE](#) in the SQL Server documentation.
7. If you are creating database users in the script, check to see if server logins exist on the target DB instance for those users. If not, create logins for those users; the scripted commands to create the database users fail otherwise. For more information, see [Create a login](#) in the SQL Server documentation.
8. Choose **!Execute** on the SQL Editor menu to run the script file and create the database objects. When the script finishes, verify that all database objects exist as expected.
9. Use the bcp utility to export data from the RDS for SQL Server DB instance into files. Open a command prompt and type the following command.

```
bcp database_name.schema_name.table_name out data_file -n -S aws_rds_sql_endpoint -U
username -P password
```

The preceding code includes the following options:

- *table_name* is the name of one of the tables that you've recreated in the target database and now want to populate with data.
- *data_file* is the full path and name of the data file to be created.
- *-n* specifies that the bulk copy uses the native data types of the data to be copied.
- *-S* specifies the SQL Server DB instance to export from.
- *-U* specifies the user name to use when connecting to the SQL Server DB instance.
- *-P* specifies the password for the user specified by *-U*.

The following shows an example command.

```
bcp world.dbo.city out C:\Users\JohnDoe\city.dat -n -S sql-jdoe.1234abcd.us-
west-2.rds.amazonaws.com,1433 -U JohnDoe -P ClearTextPassword
```

Repeat this step until you have data files for all of the tables you want to export.

10. Prepare your target DB instance for bulk import of data by following the instructions at [Basic guidelines for bulk importing data](#) in the SQL Server documentation.
11. Decide on a bulk import method to use after considering performance and other concerns discussed in [About bulk import and bulk export operations](#) in the SQL Server documentation.
12. Bulk import the data from the data files that you created using the bcp utility. To do so, follow the instructions at either [Import and export bulk data by using the bcp utility](#) or [Import bulk data by using BULK INSERT or OPENROWSET\(BULK...\)](#) in the SQL Server documentation, depending on what you decided in step 11.

Working with read replicas for Microsoft SQL Server in Amazon RDS

You usually use read replicas to configure replication between Amazon RDS DB instances. For general information about read replicas, see [Working with read replicas \(p. 370\)](#).

In this section, you can find specific information about working with read replicas on Amazon RDS for SQL Server.

Topics

- [Configuring read replicas for SQL Server \(p. 1126\)](#)
- [Read replica limitations with SQL Server \(p. 1126\)](#)
- [Option considerations for RDS for SQL Server replicas \(p. 1127\)](#)
- [Troubleshooting a SQL Server read replica problem \(p. 1128\)](#)

Configuring read replicas for SQL Server

Before a DB instance can serve as a source instance for replication, you must enable automatic backups on the source DB instance. To do so, you set the backup retention period to a value other than 0. The source DB instance must be a Multi-AZ deployment with Always On Availability Groups (AGs). Setting this type of deployment also enforces that automatic backups are enabled.

Creating a SQL Server read replica doesn't require an outage for the primary DB instance. Amazon RDS sets the necessary parameters and permissions for the source DB instance and the read replica without any service interruption. A snapshot is taken of the source DB instance, and this snapshot becomes the read replica. No outage occurs when you delete a read replica.

You can create up to five read replicas from one source DB instance. For replication to operate effectively, we recommend that you configure each read replica with the same amount of compute and storage resources as the source DB instance. If you scale the source DB instance, also scale the read replicas.

The SQL Server DB engine version of the source DB instance and all of its read replicas must be the same. Amazon RDS upgrades the primary immediately after upgrading the read replicas, regardless of the maintenance window. For more information about upgrading the DB engine version, see [Upgrading the Microsoft SQL Server DB engine \(p. 1094\)](#).

For a read replica to receive and apply changes from the source, it should have sufficient compute and storage resources. If a read replica reaches compute, network, or storage resource capacity, the read replica stops receiving or applying changes from its source. You can modify the storage and CPU resources of a read replica independently from its source and other read replicas.

Read replica limitations with SQL Server

The following limitations apply to SQL Server read replicas on Amazon RDS:

- Read replicas are only available on the SQL Server Enterprise Edition (EE) engine.
- Read replicas are available for SQL Server versions 2016–2019.
- The source DB instance to be replicated must be a Multi-AZ deployment with Always On AGs.
- Read replicas are only available for DB instances running on DB instance classes with four or more vCPUs.
- The following aren't supported on Amazon RDS for SQL Server:

- Backup retention of read replicas
- Point-in-time recovery from read replicas
- Manual snapshots of read replicas
- Multi-AZ read replicas
- Creating read replicas of read replicas
- Synchronization of user logins to read replicas
- Amazon RDS for SQL Server doesn't intervene to mitigate high replica lag between a source DB instance and its read replicas. Make sure that the source DB instance and its read replicas are sized properly, in terms of computing power and storage, to suit their operational load.

Option considerations for RDS for SQL Server replicas

Before you create an RDS for SQL Server replica, consider the following requirements, restrictions, and recommendations:

- If your SQL Server replica is in the same Region as its source DB instance, make sure that it belongs to the same option group as the source DB instance. Modifications to the source option group or source option group membership propagate to replicas. These changes are applied to the replicas immediately after they are applied to the source DB instance, regardless of the replica's maintenance window.

For more information about option groups, see [Working with option groups \(p. 273\)](#).

- When you create a SQL Server cross-Region replica, Amazon RDS creates a dedicated option group for it.

You can't remove an SQL Server cross-Region replica from its dedicated option group. No other DB instances can use the dedicated option group for a SQL Server cross-Region replica.

The following options are replicated options. To add replicated options to a SQL Server cross-Region replica, add it to the source DB instance's option group. The option is also installed on all of the source DB instance's replicas.

- TDE

The following options are non-replicated options. You can add or remove non-replicated options from a dedicated option group.

- MSDTC
- SQLSERVER_AUDIT
- To enable the SQLSERVER_AUDIT option on cross-Region read replica, add the SQLSERVER_AUDIT option on the dedicated option group on the cross-region read replica and the source instance's option group. By adding the SQLSERVER_AUDIT option on the source instance of SQL Server cross-Region read replica, you can create Server Level Audit Object and Server Level Audit Specifications on each of the cross-Region read replicas of the source instance. To allow the cross-Region read replicas access to upload the completed audit logs to an Amazon S3 bucket, add the SQLSERVER_AUDIT option to the dedicated option group and configure the option settings. The Amazon S3 bucket that you use as a target for audit files must be in the same Region as the cross-Region read replica. You can modify the option setting of the SQLSERVER_AUDIT option for each cross region read replica independently so each can access an Amazon S3 bucket in their respective Region.

The following options are not supported for cross-Region read replicas.

- SSRS
- SSAS
- SSIS

The following options are partially supported for cross-Region read replicas.

- SQLSERVER_BACKUP_RESTORE
- The source DB instance of a SQL Server cross-Region replica can have the SQLSERVER_BACKUP_RESTORE option, but you can not perform native restores on the source DB instance until you delete all its cross-Region replicas. Any existing native restore tasks will be cancelled during the creation of a cross-Region replica. You can't add the SQLSERVER_BACKUP_RESTORE option to a dedicated option group.

For more information on native backup and restore, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#)

When you promote a SQL Server cross-Region read replica, the promoted replica behaves the same as other SQL Server DB instances, including the management of its options. For more information about option groups, see [Working with option groups \(p. 273\)](#).

Troubleshooting a SQL Server read replica problem

You can monitor replication lag in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric. For information about replication lag time, see [Monitoring read replication \(p. 380\)](#).

If replication lag is too long, you can use the following query to get information about the lag.

```
SELECT AR.replica_server_name
    , DB_NAME(ARS.database_id) 'database_name'
    , AR.availability_mode_desc
    , ARS.synchronization_health_desc
    , ARS.last_hardened_lsn
    , ARS.last_redone_lsn
    , ARS.secondary_lag_seconds
FROM sys.dm_hadr_database_replica_states ARS
INNER JOIN sys.availability_replicas AR ON ARS.replica_id = AR.replica_id
--WHERE DB_NAME(ARS.database_id) = 'database_name'
ORDER BY AR.replica_server_name;
```

Multi-AZ deployments for Amazon RDS for Microsoft SQL Server

Multi-AZ deployments provide increased availability, data durability, and fault tolerance for DB instances. In the event of planned database maintenance or unplanned service disruption, Amazon RDS automatically fails over to the up-to-date secondary DB instance. This functionality lets database operations resume quickly without manual intervention. The primary and standby instances use the same endpoint, whose physical network address transitions to the secondary replica as part of the failover process. You don't have to reconfigure your application when a failover occurs.

Amazon RDS supports Multi-AZ deployments for Microsoft SQL Server by using either SQL Server Database Mirroring (DBM) or Always On Availability Groups (AGs). Amazon RDS monitors and maintains the health of your Multi-AZ deployment. If problems occur, RDS automatically repairs unhealthy DB instances, reestablishes synchronization, and initiates failovers. Failover only occurs if the standby and primary are fully in sync. You don't have to manage anything.

When you set up SQL Server Multi-AZ, RDS automatically configures all databases on the instance to use DBM or AGs. Amazon RDS handles the primary, the witness, and the secondary DB instance for you. Because configuration is automatic, RDS selects DBM or Always On AGs based on the version of SQL Server that you deploy.

Amazon RDS supports Multi-AZ with Always On AGs for the following SQL Server versions and editions:

- SQL Server 2019:
 - Standard Edition 15.00.4073.23 and higher
 - Enterprise Edition
- SQL Server 2017:
 - Standard Edition 14.00.3401.7 and higher
 - Enterprise Edition 14.00.3049.1 and higher
- SQL Server 2016: Enterprise Edition 13.00.5216.0 and higher

Amazon RDS supports Multi-AZ with DBM for the following SQL Server versions and editions, except for the versions noted previously:

- SQL Server 2019: Standard Edition 15.00.4043.16
- SQL Server 2017: Standard and Enterprise Editions
- SQL Server 2016: Standard and Enterprise Editions
- SQL Server 2014: Standard and Enterprise Editions

You can use the following SQL query to determine whether your SQL Server DB instance is Single-AZ, Multi-AZ with DBM, or Multi-AZ with Always On AGs.

```
SELECT CASE WHEN dm.mirroring_state_desc IS NOT NULL THEN 'Multi-AZ (Mirroring)'  
WHEN dhdrs.group_database_id IS NOT NULL THEN 'Multi-AZ (AlwaysOn)'  
ELSE 'Single-AZ'  
END 'high_availability'  
FROM sys.databases sd  
LEFT JOIN sys.database_mirroring dm ON sd.database_id = dm.database_id  
LEFT JOIN sys.dm_hadr_database_replica_states dhdrs ON sd.database_id = dhdrs.database_id  
AND dhdrs.is_local = 1  
WHERE DB_NAME(sd.database_id) = 'rdsadmin';
```

The output resembles the following:

```
high_availability  
Multi-AZ (AlwaysOn)
```

Adding Multi-AZ to a Microsoft SQL Server DB instance

When you create a new SQL Server DB instance using the AWS Management Console, you can add Multi-AZ with Database Mirroring (DBM) or Always On AGs. You do so by choosing **Yes (Mirroring / Always On)** from **Multi-AZ deployment**. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

When you modify an existing SQL Server DB instance using the console, you can add Multi-AZ with DBM or AGs by choosing **Yes (Mirroring / Always On)** from **Multi-AZ deployment** on the **Modify DB instance** page. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

If your DB instance is running Database Mirroring (DBM)—not Always On Availability Groups (AGs)—you might need to disable in-memory optimization before you add Multi-AZ. Disable in-memory optimization with DBM before you add Multi-AZ if your DB instance runs SQL Server 2014, 2016, or 2017 Enterprise Edition and has in-memory optimization enabled.

If your DB instance is running AGs, it doesn't require this step.

Removing Multi-AZ from a Microsoft SQL Server DB instance

When you modify an existing SQL Server DB instance using the AWS Management Console, you can remove Multi-AZ with DBM or AGs. You can do this by choosing **No (Mirroring / Always On)** from **Multi-AZ deployment** on the **Modify DB instance** page. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Microsoft SQL Server Multi-AZ deployment limitations, notes, and recommendations

The following are some limitations when working with Multi-AZ deployments on RDS for SQL Server DB instances:

- Cross-Region Multi-AZ isn't supported.
- You can't configure the secondary DB instance to accept database read activity.
- Multi-AZ with Always On Availability Groups (AGs) supports in-memory optimization.
- Multi-AZ with Always On Availability Groups (AGs) doesn't support Kerberos authentication for the availability group listener. This is because the listener has no Service Principal Name (SPN).
- You can't rename a database on a SQL Server DB instance that is in a SQL Server Multi-AZ deployment. If you need to rename a database on such an instance, first turn off Multi-AZ for the DB instance, then rename the database. Finally, turn Multi-AZ back on for the DB instance.
- You can only restore Multi-AZ DB instances that are backed up using the full recovery model.
- Multi-AZ deployments have a limit of 100 SQL Server Agent jobs.

If you need a higher limit, request an increase by contacting AWS Support. Open the [AWS Support Center](#) page, sign in if necessary, and choose **Create case**. Choose **Service limit increase**. Complete and submit the form.

The following are some notes about working with Multi-AZ deployments on RDS for SQL Server DB instances:

- Amazon RDS exposes the Always On AGs [availability group listener endpoint](#). The endpoint is visible in the console, and is returned by the `DescribeDBInstances` API operation as an entry in the `Endpoints` field.
- Amazon RDS supports [availability group multisubnet failovers](#).
- To use SQL Server Multi-AZ with a SQL Server DB instance in a virtual private cloud (VPC), first create a DB subnet group that has subnets in at least two distinct Availability Zones. Then assign the DB subnet group to the primary replica of the SQL Server DB instance.
- When a DB instance is modified to be a Multi-AZ deployment, during the modification it has a status of **modifying**. Amazon RDS creates the standby, and makes a backup of the primary DB instance. After the process is complete, the status of the primary DB instance becomes **available**.
- Multi-AZ deployments maintain all databases on the same node. If a database on the primary host fails over, all your SQL Server databases fail over as one atomic unit to your standby host. Amazon RDS provisions a new healthy host, and replaces the unhealthy host.
- Multi-AZ with DBM or AGs supports a single standby replica.
- Users, logins, and permissions are automatically replicated for you on the secondary. You don't need to recreate them. User-defined server roles are only replicated in DB instances that use Always On AGs for Multi-AZ deployments.
- In Multi-AZ deployments, SQL Server Agent jobs are replicated from the primary host to the secondary host when the job replication feature is turned on. For more information, see [Turning on SQL Server Agent job replication \(p. 1306\)](#).
- You might observe elevated latencies compared to a standard DB instance deployment (in a single Availability Zone) because of the synchronous data replication.
- Failover times are affected by the time it takes to complete the recovery process. Large transactions increase the failover time.
- In SQL Server Multi-AZ deployments, reboot with failover reboots only the primary DB instance. After the failover, the primary DB instance becomes the new secondary DB instance. Parameters might not be updated for Multi-AZ instances. For reboot without failover, both the primary and secondary DB instances reboot, and parameters are updated after the reboot. If the DB instance is unresponsive, we recommend reboot without failover.

The following are some recommendations for working with Multi-AZ deployments on RDS for Microsoft SQL Server DB instances:

- For databases used in production or preproduction, we recommend the following options:
 - Multi-AZ deployments for high availability
 - "Provisioned IOPS" for fast, consistent performance
 - "Memory optimized" rather than "General purpose"
- You can't select the Availability Zone (AZ) for the secondary instance, so when you deploy application hosts, take this into account. Your database might fail over to another AZ, and the application hosts might not be in the same AZ as the database. For this reason, we recommend that you balance your application hosts across all AZs in the given AWS Region.
- For best performance, don't enable Database Mirroring or Always On AGs during a large data load operation. If you want your data load to be as fast as possible, finish loading data before you convert your DB instance to a Multi-AZ deployment.
- Applications that access the SQL Server databases should have exception handling that catches connection errors. The following code sample shows a try/catch block that catches a communication error. In this example, the break statement exits the while loop if the connection is successful, but retries up to 10 times if an exception is thrown.

```
int RetryMaxAttempts = 10;
int RetryIntervalPeriodInSeconds = 1;
int iRetryCount = 0;
while (iRetryCount < RetryMaxAttempts)
{
    using (SqlConnection connection = new SqlConnection(DatabaseConnectionString))
    {
        using (SqlCommand command = connection.CreateCommand())
        {
            command.CommandText = "INSERT INTO SOME_TABLE VALUES ('SomeValue');";
            try
            {
                connection.Open();
                command.ExecuteNonQuery();
                break;
            }
            catch (Exception ex)
            {
                Logger(ex.Message);
                iRetryCount++;
            }
            finally {
                connection.Close();
            }
        }
    }
    Thread.Sleep(RetryIntervalPeriodInSeconds * 1000);
}
```

- Don't use the `SET PARTNER OFF` command when working with Multi-AZ instances. For example, don't do the following.

```
--Don't do this
ALTER DATABASE db1 SET PARTNER off
```

- Don't set the recovery mode to `simple`. For example, don't do the following.

```
--Don't do this
ALTER DATABASE db1 SET RECOVERY simple
```

- Don't use the `DEFAULT_DATABASE` parameter when creating new logins on Multi-AZ DB instances, because these settings can't be applied to the standby mirror. For example, don't do the following.

```
--Don't do this
CREATE LOGIN [test_dba] WITH PASSWORD=foo, DEFAULT_DATABASE=[db2]
```

Also, don't do the following.

```
--Don't do this
ALTER LOGIN [test_dba] SET DEFAULT_DATABASE=[db3]
```

Determining the location of the secondary

You can determine the location of the secondary replica by using the AWS Management Console. You need to know the location of the secondary if you are setting up your primary DB instance in a VPC.

Configuration	Instance class	Storage
DB instance id database-1	Instance class db.m4.large	Encryption Enabled
Engine version 14.00.3192.2.v1	vCPU 2	KMS key aws/rds
DB name -	RAM 8 GB	Storage type General Purpose (SSD)
License model License Included	Availability	IOPS -
Collation SQL_Latin1_General_CI_AS	Master username admin	Storage 20 GiB
Option groups default:sqserver-se-14-00	IAM db authentication Not Enabled	Storage autoscaling Enabled
ARN arn:aws:rds:us-west-2: db:database-1	Multi AZ Yes (Mirroring)	Maximum storage threshold 1000 GiB
Resource id db- [REDACTED]	Secondary Zone us-west-2c	

You can also view the Availability Zone of the secondary using the AWS CLI command `describe-db-instances` or RDS API operation `DescribeDBInstances`. The output shows the secondary AZ where the standby mirror is located.

Migrating from Database Mirroring to Always On Availability Groups

In version 14.00.3049.1 of Microsoft SQL Server Enterprise Edition, Always On Availability Groups (AGs) are enabled by default.

To migrate from Database Mirroring (DBM) to AGs, first check your version. If you are using a DB instance with a version prior to Enterprise Edition 13.00.5216.0, modify the instance to patch it to 13.00.5216.0 or later. If you are using a DB instance with a version prior to Enterprise Edition 14.00.3049.1, modify the instance to patch it to 14.00.3049.1 or later.

If you want to upgrade a mirrored DB instance to use AGs, run the upgrade first, modify the instance to remove Multi-AZ, and then modify it again to add Multi-AZ. This converts your instance to use Always On AGs.

Additional features for Microsoft SQL Server on Amazon RDS

In the following sections, you can find information about augmenting Amazon RDS instances running the Microsoft SQL Server DB engine.

Topics

- [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#)
- [Configuring security protocols and ciphers \(p. 1138\)](#)
- [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#)
- [Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 \(p. 1153\)](#)
- [Using Database Mail on Amazon RDS for SQL Server \(p. 1167\)](#)
- [Instance store support for the tempdb database on Amazon RDS for SQL Server \(p. 1178\)](#)
- [Using extended events with Amazon RDS for Microsoft SQL Server \(p. 1180\)](#)
- [Access to transaction log backups with RDS for SQL Server \(p. 1183\)](#)

Using SSL with a Microsoft SQL Server DB instance

You can use Secure Sockets Layer (SSL) to encrypt connections between your client applications and your Amazon RDS DB instances running Microsoft SQL Server. SSL support is available in all AWS regions for all supported SQL Server editions.

When you create a SQL Server DB instance, Amazon RDS creates an SSL certificate for it. The SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

There are 2 ways to use SSL to connect to your SQL Server DB instance:

- Force SSL for all connections — this happens transparently to the client, and the client doesn't have to do any work to use SSL.
- Encrypt specific connections — this sets up an SSL connection from a specific client computer, and you must do work on the client to encrypt connections.

For information about Transport Layer Security (TLS) support for SQL Server, see [TLS 1.2 support for Microsoft SQL Server](#).

Forcing connections to your DB instance to use SSL

You can force all connections to your DB instance to use SSL. If you force connections to use SSL, it happens transparently to the client, and the client doesn't have to do any work to use SSL.

If you want to force SSL, use the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to `0` (off). Set the `rds.force_ssl` parameter to `1` (on) to force connections to use SSL. The `rds.force_ssl` parameter is static, so after you change the value, you must reboot your DB instance for the change to take effect.

To force all connections to your DB instance to use SSL

1. Determine the parameter group that is attached to your DB instance:
 - a. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
 - b. In the top right corner of the Amazon RDS console, choose the AWS Region of your DB instance.
 - c. In the navigation pane, choose **Databases**, and then choose the name of your DB instance to show its details.
 - d. Choose the **Configuration** tab. Find the **Parameter group** in the section.
2. If necessary, create a new parameter group. If your DB instance uses the default parameter group, you must create a new parameter group. If your DB instance uses a nondefault parameter group, you can choose to edit the existing parameter group or to create a new parameter group. If you edit an existing parameter group, the change affects all DB instances that use that parameter group.

To create a new parameter group, follow the instructions in [Creating a DB parameter group \(p. 291\)](#).

3. Edit your new or existing parameter group to set the `rds.force_ssl` parameter to `true`. To edit the parameter group, follow the instructions in [Modifying parameters in a DB parameter group \(p. 294\)](#).
4. If you created a new parameter group, modify your DB instance to attach the new parameter group. Modify the **DB Parameter Group** setting of the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
5. Reboot your DB instance. For more information, see [Rebooting a DB instance \(p. 366\)](#).

Encrypting specific connections

You can force all connections to your DB instance to use SSL, or you can encrypt connections from specific client computers only. To use SSL from a specific client, you must obtain certificates for the client computer, import certificates on the client computer, and then encrypt the connections from the client computer.

Note

All SQL Server instances created after August 5, 2014, use the DB instance endpoint in the Common Name (CN) field of the SSL certificate. Prior to August 5, 2014, SSL certificate verification was not available for VPC-based SQL Server instances. If you have a VPC-based SQL Server DB instance that was created before August 5, 2014, and you want to use SSL certificate verification and ensure that the instance endpoint is included as the CN for the SSL certificate for that DB instance, then rename the instance. When you rename a DB instance, a new certificate is deployed and the instance is rebooted to enable the new certificate.

Obtaining certificates for client computers

To encrypt connections from a client computer to an Amazon RDS DB instance running Microsoft SQL Server, you need a certificate on your client computer.

To obtain that certificate, download the certificate to your client computer. You can download a root certificate that works for all regions. You can also download a certificate bundle that contains both the old and new root certificate. In addition, you can download region-specific intermediate certificates. For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

After you have downloaded the appropriate certificate, import the certificate into your Microsoft Windows operating system by following the procedure in the section following.

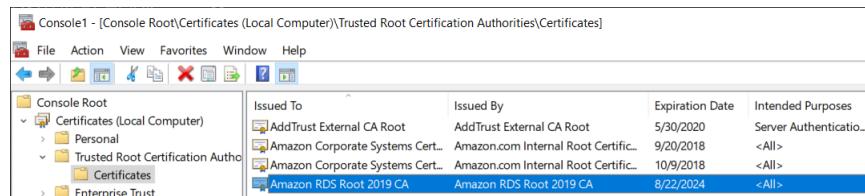
Importing certificates on client computers

You can use the following procedure to import your certificate into the Microsoft Windows operating system on your client computer.

To import the certificate into your Windows operating system:

1. On the **Start** menu, type **Run** in the search box and press **Enter**.
2. In the **Open** box, type **MMC** and then choose **OK**.
3. In the MMC console, on the **File** menu, choose **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog box, for **Available snap-ins**, select **Certificates**, and then choose **Add**.
5. In the **Certificates snap-in** dialog box, choose **Computer account**, and then choose **Next**.
6. In the **Select computer** dialog box, choose **Finish**.
7. In the **Add or Remove Snap-ins** dialog box, choose **OK**.
8. In the MMC console, expand **Certificates**, open the context (right-click) menu for **Trusted Root Certification Authorities**, choose **All Tasks**, and then choose **Import**.
9. On the first page of the Certificate Import Wizard, choose **Next**.
10. On the second page of the Certificate Import Wizard, choose **Browse**. In the browse window, change the file type to **All files (*.*)** because .pem is not a standard certificate extension. Locate the .pem file that you downloaded previously.
11. Choose **Open** to select the certificate file, and then choose **Next**.
12. On the third page of the Certificate Import Wizard, choose **Next**.
13. On the fourth page of the Certificate Import Wizard, choose **Finish**. A dialog box appears indicating that the import was successful.

14. In the MMC console, expand **Certificates**, expand **Trusted Root Certification Authorities**, and then choose **Certificates**. Locate the certificate to confirm it exists, as shown here.



Encrypting connections to an Amazon RDS DB instance running Microsoft SQL Server

After you have imported a certificate into your client computer, you can encrypt connections from the client computer to an Amazon RDS DB instance running Microsoft SQL Server.

For SQL Server Management Studio, use the following procedure. For more information about SQL Server Management Studio, see [Use SQL Server management studio](#).

To encrypt connections from SQL Server Management Studio

1. Launch SQL Server Management Studio.
2. For **Connect to server**, type the server information, login user name, and password.
3. Choose **Options**.
4. Select **Encrypt connection**.
5. Choose **Connect**.
6. Confirm that your connection is encrypted by running the following query. Verify that the query returns true for `encrypt_option`.

```
select ENCRYPT_OPTION from SYS.DM_EXEC_CONNECTIONS where SESSION_ID = @@SPID
```

For any other SQL client, use the following procedure.

To encrypt connections from other SQL clients

1. Append `encrypt=true` to your connection string. This string might be available as an option, or as a property on the connection page in GUI tools.

Note

To enable SSL encryption for clients that connect using JDBC, you might need to add the Amazon RDS SQL certificate to the Java CA certificate (cacerts) store. You can do this by using the `keytool` utility.

2. Confirm that your connection is encrypted by running the following query. Verify that the query returns true for `encrypt_option`.

```
select ENCRYPT_OPTION from SYS.DM_EXEC_CONNECTIONS where SESSION_ID = @@SPID
```

Configuring security protocols and ciphers

You can turn certain security protocols and ciphers on and off using DB parameters. The security parameters that you can configure (except for TLS version 1.2) are shown in the following table.

For parameters other than `rds.fips`, the value of default means that the operating system default value is used, whether it is enabled or disabled.

Note

You can't disable TLS 1.2, because Amazon RDS uses it internally.

DB parameter	Allowed values (default in bold)	Description
<code>rds.tls10</code>	default , enabled, disabled	TLS 1.0.
<code>rds.tls11</code>	default , enabled, disabled	TLS 1.1.
<code>rds.tls12</code>	default	TLS 1.2. You can't modify this value.
<code>rds.fips</code>	0 , 1	<p>When you set the parameter to 1, RDS forces the use of modules that are compliant with the Federal Information Processing Standard (FIPS) 140-2 standard.</p> <p>For more information, see Use SQL Server 2016 in FIPS 140-2-compliant mode in the Microsoft documentation.</p> <p>Note You must reboot the DB instance after the modification to make it effective.</p>
<code>rds.rc4</code>	default , enabled, disabled	RC4 stream cipher.
<code>rds.diffie-hellman</code>	default , enabled, disabled	Diffie-Hellman key-exchange encryption.
<code>rds.diffie-hellman-min-key-bit-length</code>	default , 1024, 2048, 4096	Minimum bit length for Diffie-Hellman keys.
<code>rds.curve25519</code>	default , enabled, disabled	Curve25519 elliptic-curve encryption cipher. This parameter isn't supported for all engine versions.
<code>rds.3des168</code>	default , enabled, disabled	Triple Data Encryption Standard (DES) encryption cipher with a 168-bit key length.

Note

For more information on the default values for SQL Server security protocols and ciphers, see [Protocols in TLS/SSL \(Schannel SSP\)](#) and [Cipher Suites in TLS/SSL \(Schannel SSP\)](#) in the Microsoft documentation.

For more information on viewing and setting these values in the Windows Registry, see [Transport Layer Security \(TLS\) best practices with the .NET Framework](#) in the Microsoft documentation.

Use the following process to configure the security protocols and ciphers:

1. Create a custom DB parameter group.
2. Modify the parameters in the parameter group.
3. Associate the DB parameter group with your DB instance.

For more information on DB parameter groups, see [Working with parameter groups \(p. 289\)](#).

Creating the security-related parameter group

Create a parameter group for your security-related parameters that corresponds to the SQL Server edition and version of your DB instance.

Console

The following procedure creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.
4. In the **Create parameter group** pane, do the following:
 - a. For **Parameter group family**, choose **sqlserver-se-13.0**.
 - b. For **Group name**, enter an identifier for the parameter group, such as **sqlserver-ciphers-se-13**.
 - c. For **Description**, enter **Parameter group for security protocols and ciphers**.
5. Choose **Create**.

CLI

The following procedure creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
--db-parameter-group-name sqlserver-ciphers-se-13 \
--db-parameter-group-family "sqlserver-se-13.0" \
```

```
--description "Parameter group for security protocols and ciphers"
```

For Windows:

```
aws rds create-db-parameter-group ^
--db-parameter-group-name sqlserver-ciphers-se-13 ^
--db-parameter-group-family "sqlserver-se-13.0" ^
--description "Parameter group for security protocols and ciphers"
```

Modifying security-related parameters

Modify the security-related parameters in the parameter group that corresponds to the SQL Server edition and version of your DB instance.

Console

The following procedure modifies the parameter group that you created for SQL Server Standard Edition 2016. This example turns off TLS version 1.0.

To modify the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group, such as **sqlserver-ciphers-se-13**.
4. Under **Parameters**, filter the parameter list for **rds**.
5. Choose **Edit parameters**.
6. Choose **rds.tls10**.
7. For **Values**, choose **disabled**.
8. Choose **Save changes**.

CLI

The following procedure modifies the parameter group that you created for SQL Server Standard Edition 2016. This example turns off TLS version 1.0.

To modify the parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name sqlserver-ciphers-se-13 \
--parameters
"ParameterName='rds.tls10',ParameterValue='disabled',ApplyMethod=pending-reboot"
```

For Windows:

```
aws rds modify-db-parameter-group ^
```

```
--db-parameter-group-name sqlserver-ciphers-se-13 ^
--parameters
"ParameterName='rds.tls10',ParameterValue='disabled',ApplyMethod=pending-reboot"
```

Associating the security-related parameter group with your DB instance

To associate the parameter group with your DB instance, use the AWS Management Console or the AWS CLI.

Console

You can associate the parameter group with a new or existing DB instance:

- For a new DB instance, associate it when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, associate it by modifying the instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

You can associate the parameter group with a new or existing DB instance.

To create a DB instance with the parameter group

- Specify the same DB engine type and major version as you used when creating the parameter group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier mydbinstance \
--db-instance-class db.m5.2xlarge \
--engine sqlserver-se \
--engine-version 13.00.5426.0.v1 \
--allocated-storage 100 \
--master-user-password secret123 \
--master-username admin \
--storage-type gp2 \
--license-model li \
--db-parameter-group-name sqlserver-ciphers-se-13
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--db-instance-class db.m5.2xlarge ^
--engine sqlserver-se ^
--engine-version 13.00.5426.0.v1 ^
--allocated-storage 100 ^
--master-user-password secret123 ^
--master-username admin ^
--storage-type gp2 ^
--license-model li ^
--db-parameter-group-name sqlserver-ciphers-se-13
```

To modify a DB instance and associate the parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-parameter-group-name sqlserver-ciphers-se-13 \
    --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-parameter-group-name sqlserver-ciphers-se-13 ^
    --apply-immediately
```

Using Windows Authentication with an Amazon RDS for SQL Server DB instance

You can use Microsoft Windows Authentication to authenticate users when they connect to your Amazon RDS for Microsoft SQL Server DB instance. The DB instance works with AWS Directory Service for Microsoft Active Directory, also called AWS Managed Microsoft AD, to enable Windows Authentication. When users authenticate with a SQL Server DB instance joined to the trusting domain, authentication requests are forwarded to the domain directory that you create with AWS Directory Service.

Region and version availability

Amazon RDS supports Windows Authentication for SQL Server in all AWS Regions. RDS supports using only AWS Managed Microsoft AD for Windows Authentication. RDS doesn't support using AD Connector. For more information, see the following:

- [Application compatibility policy for AWS Managed Microsoft AD](#)
- [Application compatibility policy for AD Connector](#)

For more information on version and Region availability of RDS for SQL Server with Kerberos authentication, see [Kerberos authentication \(p. 101\)](#).

Overview of setting up Windows authentication

To set up Windows authentication, complete the following general steps, described in more detail later:

Amazon RDS uses mixed mode for Windows Authentication. This approach means that the *master user* (the name and password used to create your SQL Server DB instance) uses SQL Authentication. Because the master user account is a privileged credential, you should restrict access to this account.

To get Windows Authentication using an on-premises or self-hosted Microsoft Active Directory, create a forest trust. The trust can be one-way or two-way. For more information on setting up forest trusts using AWS Directory Service, see [When to create a trust relationship in the AWS Directory Service Administration Guide](#).

To set up Windows authentication for a SQL Server DB instance, do the following steps, explained in greater detail in [Setting up Windows Authentication for SQL Server DB instances \(p. 1144\)](#):

1. Use AWS Managed Microsoft AD, either from the AWS Management Console or AWS Directory Service API, to create an AWS Managed Microsoft AD directory.
2. If you use the AWS CLI or Amazon RDS API to create your SQL Server DB instance, create an AWS Identity and Access Management (IAM) role. This role uses the managed IAM policy `AmazonRDSDirectoryServiceAccess` and allows Amazon RDS to make calls to your directory. If you use the console to create your SQL Server DB instance, AWS creates the IAM role for you.

For the role to allow access, the AWS Security Token Service (AWS STS) endpoint must be activated in the AWS Region for your AWS account. AWS STS endpoints are active by default in all AWS Regions, and you can use them without any further actions. For more information, see [Managing AWS STS in an AWS Region](#) in the [IAM User Guide](#).

3. Create and configure users and groups in the AWS Managed Microsoft AD directory using the Microsoft Active Directory tools. For more information about creating users and groups in your Active Directory, see [Manage users and groups in AWS Managed Microsoft AD](#) in the [AWS Directory Service Administration Guide](#).
4. If you plan to locate the directory and the DB instance in different VPCs, enable cross-VPC traffic.
5. Use Amazon RDS to create a new SQL Server DB instance either from the console, AWS CLI, or Amazon RDS API. In the create request, you provide the domain identifier ("d-*" identifier) that was generated

when you created your directory and the name of the role you created. You can also modify an existing SQL Server DB instance to use Windows Authentication by setting the domain and IAM role parameters for the DB instance.

6. Use the Amazon RDS master user credentials to connect to the SQL Server DB instance as you do any other DB instance. Because the DB instance is joined to the AWS Managed Microsoft AD domain, you can provision SQL Server logins and users from the Active Directory users and groups in their domain. (These are known as SQL Server "Windows" logins.) Database permissions are managed through standard SQL Server permissions granted and revoked to these Windows logins.

Creating the endpoint for Kerberos authentication

Kerberos-based authentication requires that the endpoint be the customer-specified host name, a period, and then the fully qualified domain name (FQDN). For example, the following is an example of an endpoint you might use with Kerberos-based authentication. In this example, the SQL Server DB instance host name is ad-test and the domain name is corp-ad.company.com.

```
ad-test.corp-ad.company.com
```

If you want to make sure your connection is using Kerberos, run the following query:

```
SELECT net_transport, auth_scheme
  FROM sys.dm_exec_connections
 WHERE session_id = @@SPID;
```

Setting up Windows Authentication for SQL Server DB instances

You use AWS Directory Service for Microsoft Active Directory, also called AWS Managed Microsoft AD, to set up Windows Authentication for a SQL Server DB instance. To set up Windows Authentication, take the following steps.

Step 1: Create a directory using the AWS Directory Service for Microsoft Active Directory

AWS Directory Service creates a fully managed, Microsoft Active Directory in the AWS Cloud. When you create an AWS Managed Microsoft AD directory, AWS Directory Service creates two domain controllers and Domain Name Service (DNS) servers on your behalf. The directory servers are created in two subnets in two different Availability Zones within a VPC. This redundancy helps ensure that your directory remains accessible even if a failure occurs.

When you create an AWS Managed Microsoft AD directory, AWS Directory Service performs the following tasks on your behalf:

- Sets up a Microsoft Active Directory within the VPC.
- Creates a directory administrator account with the user name Admin and the specified password. You use this account to manage your directory.

Note

Be sure to save this password. AWS Directory Service doesn't store this password, and you can't retrieve or reset it.

- Creates a security group for the directory controllers.

When you launch an AWS Directory Service for Microsoft Active Directory, AWS creates an Organizational Unit (OU) that contains all your directory's objects. This OU, which has the NetBIOS name that you typed when you created your directory, is located in the domain root. The domain root is owned and managed by AWS.

The *admin* account that was created with your AWS Managed Microsoft AD directory has permissions for the most common administrative activities for your OU:

- Create, update, or delete users, groups, and computers.
- Add resources to your domain such as file or print servers, and then assign permissions for those resources to users and groups in your OU.
- Create additional OUs and containers.
- Delegate authority.
- Create and link group policies.
- Restore deleted objects from the Active Directory Recycle Bin.
- Run AD and DNS Windows PowerShell modules on the Active Directory Web Service.

The admin account also has rights to perform the following domain-wide activities:

- Manage DNS configurations (add, remove, or update records, zones, and forwarders).
- View DNS event logs.
- View security event logs.

To create a directory with AWS Managed Microsoft AD

1. In the [AWS Directory Service console](#) navigation pane, choose **Directories** and choose **Set up directory**.
2. Choose **AWS Managed Microsoft AD**. This is the only option currently supported for use with Amazon RDS.
3. Choose **Next**.
4. On the **Enter directory information** page, provide the following information:

Edition

Choose the edition that meets your requirements.

Directory DNS name

The fully qualified name for the directory, such as `corp.example.com`. Names longer than 47 characters aren't supported by SQL Server.

Directory NetBIOS name

An optional short name for the directory, such as `CORP`.

Directory description

An optional description for the directory.

Admin password

The password for the directory administrator. The directory creation process creates an administrator account with the user name `Admin` and this password.

The directory administrator password can't include the word `admin`. The password is case-sensitive and must be 8–64 characters in length. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#\$%^&*_+=`|\{};:"<>,.?/)

Confirm password

Retype the administrator password.

5. Choose **Next**.
6. On the **Choose VPC and subnets** page, provide the following information:

VPC

Choose the VPC for the directory.

Note

You can locate the directory and the DB instance in different VPCs, but if you do so, make sure to enable cross-VPC traffic. For more information, see [Step 4: Enable cross-VPC traffic between the directory and the DB instance \(p. 1149\)](#).

Subnets

Choose the subnets for the directory servers. The two subnets must be in different Availability Zones.

7. Choose **Next**.
8. Review the directory information. If changes are needed, choose **Previous**. When the information is correct, choose **Create directory**.

Review & create

Review

Directory type

Microsoft AD

Directory DNS name

corp.example.com

Directory NetBIOS name

CORP

Directory description

My directory

VPC

vpc-8b6b78e9 ([REDACTED])

Subnets

subnet-75128d10 ([REDACTED], us-east-1a)

subnet-f51665dd ([REDACTED], us-east-1b)

Pricing

Edition

Standard

Free trial eligible [Learn more](#)

30-day limited trial

~USD [REDACTED] *

* Includes two domain controllers, USD [REDACTED] /mo for each additional domain controller.

Cancel

Previous

Create directory

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to **Active**.

To see information about your directory, choose the directory ID in the directory listing. Make a note of the **Directory ID**. You need this value when you create or modify your SQL Server DB instance.

Directory details		Reset user password	
Directory type	VPC	Status	Active
Microsoft AD	vpc-6594f31c	Last updated	Tuesday, January 7, 2020
Edition	Subnets	Launch time	Tuesday, January 7, 2020
Standard	subnet-7d36a227 subnet-a2ab49c6	Availability zones	us-east-1c, us-east-1d
Directory ID	DNS address		
d-90670a8d36			
Directory DNS name	corp.example.com		
Directory NetBIOS name	CORP		
Description - Edit	My directory		
		Application management	Scale & share
		Networking & security	Maintenance

Step 2: Create the IAM role for use by Amazon RDS

If you use the console to create your SQL Server DB instance, you can skip this step. If you use the CLI or RDS API to create your SQL Server DB instance, you must create an IAM role that uses the `AmazonRDSDirectoryServiceAccess` managed IAM policy. This role allows Amazon RDS to make calls to the AWS Directory Service for you.

If you are using a custom policy for joining a domain, rather than using the AWS-managed `AmazonRDSDirectoryServiceAccess` policy, make sure that you allow the `ds:GetAuthorizedApplicationDetails` action. This requirement is effective starting July 2019, due to a change in the AWS Directory Service API.

The following IAM policy, `AmazonRDSDirectoryServiceAccess`, provides access to AWS Directory Service.

Example IAM policy for providing access to AWS Directory Service

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sts:AssumeRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::aws:policy/AmazonRDSDirectoryServiceAccess"
    }
  ]
}
```

```
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

We recommend using the [aws:SourceArn](#) and [aws:SourceAccount](#) global condition context keys in resource-based trust relationships to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the trust relationship, make sure to use the `aws:SourceArn` global condition context key with the full Amazon Resource Name (ARN) of the resources accessing the role. For Windows Authentication, make sure to include the DB instances, as shown in the following example.

Example trust relationship with global condition context key for Windows Authentication

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [
                        "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                    ]
                }
            }
        }
    ]
}
```

Create an IAM role using this IAM policy and trust relationship. For more information about creating IAM roles, see [Creating customer managed policies](#) in the *IAM User Guide*.

Step 3: Create and configure users and groups

You can create users and groups with the Active Directory Users and Computers tool. This tool is one of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. Users represent individual people or entities that have access to your directory. Groups are very useful for giving or denying privileges to groups of users, rather than having to apply those privileges to each individual user.

To create users and groups in an AWS Directory Service directory, you must be connected to a Windows EC2 instance that is a member of the AWS Directory Service directory. You must also be logged in as a user that has privileges to create users and groups. For more information, see [Add users and groups \(Simple AD and AWS Managed Microsoft AD\)](#) in the *AWS Directory Service Administration Guide*.

Step 4: Enable cross-VPC traffic between the directory and the DB instance

If you plan to locate the directory and the DB instance in the same VPC, skip this step and move on to [Step 5: Create or modify a SQL Server DB instance \(p. 1149\)](#).

If you plan to locate the directory and the DB instance in different VPCs, configure cross-VPC traffic using VPC peering or [AWS Transit Gateway](#).

The following procedure enables traffic between VPCs using VPC peering. Follow the instructions in [What is VPC peering?](#) in the *Amazon Virtual Private Cloud Peering Guide*.

To enable cross-VPC traffic using VPC peering

1. Set up appropriate VPC routing rules to ensure that network traffic can flow both ways.
2. Ensure that the DB instance's security group can receive inbound traffic from the directory's security group.
3. Ensure that there is no network access control list (ACL) rule to block traffic.

If a different AWS account owns the directory, you must share the directory.

To share the directory between AWS accounts

1. Start sharing the directory with the AWS account that the DB instance will be created in by following the instructions in [Tutorial: Sharing your AWS Managed Microsoft AD directory for seamless EC2 domain-join](#) in the *AWS Directory Service Administration Guide*.
2. Sign in to the AWS Directory Service console using the account for the DB instance, and ensure that the domain has the SHARED status before proceeding.
3. While signed into the AWS Directory Service console using the account for the DB instance, note the **Directory ID** value. You use this directory ID to join the DB instance to the domain.

Step 5: Create or modify a SQL Server DB instance

Create or modify a SQL Server DB instance for use with your directory. You can use the console, CLI, or RDS API to associate a DB instance with a directory. You can do this in one of the following ways:

- Create a new SQL Server DB instance using the console, the `create-db-instance` CLI command, or the `CreateDBInstance` RDS API operation.

For instructions, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

- Modify an existing SQL Server DB instance using the console, the `modify-db-instance` CLI command, or the `ModifyDBInstance` RDS API operation.

For instructions, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- Restore a SQL Server DB instance from a DB snapshot using the console, the `restore-db-instance-from-db-snapshot` CLI command, or the `RestoreDBInstanceFromDBSnapshot` RDS API operation.

For instructions, see [Restoring from a DB snapshot \(p. 452\)](#).

- Restore a SQL Server DB instance to a point-in-time using the console, the `restore-db-instance-to-point-in-time` CLI command, or the `RestoreDBInstanceToPointInTime` RDS API operation.

For instructions, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Windows Authentication is only supported for SQL Server DB instances in a VPC.

For the DB instance to be able to use the domain directory that you created, the following is required:

- For **Directory**, you must choose the domain identifier (d-*ID*) generated when you created the directory.
- Make sure that the VPC security group has an outbound rule that lets the DB instance communicate with the directory.

Microsoft SQL Server Windows Authentication

Choose a directory in which you want to allow authorized domain users to authenticate with this SQL Server instance using Windows Authentication.

Directory

corp.example.com (d-...)

Create a new directory

By choosing a directory and continuing with database instance creation you authorize Amazon RDS to create the IAM role necessary for using Windows Authentication

When you use the AWS CLI, the following parameters are required for the DB instance to be able to use the directory that you created:

- For the --domain parameter, use the domain identifier (d-*ID*) generated when you created the directory.
- For the --domain-iam-role-name parameter, use the role that you created that uses the managed IAM policy AmazonRDSDirectoryServiceAccess.

For example, the following CLI command modifies a DB instance to use a directory.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--domain d-ID \
--domain-iam-role-name role-name
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--domain d-ID ^
--domain-iam-role-name role-name
```

Important

If you modify a DB instance to enable Kerberos authentication, reboot the DB instance after making the change.

Step 6: Create Windows Authentication SQL Server logins

Use the Amazon RDS master user credentials to connect to the SQL Server DB instance as you do any other DB instance. Because the DB instance is joined to the AWS Managed Microsoft AD domain, you

can provision SQL Server logins and users. You do this from the Active Directory users and groups in your domain. Database permissions are managed through standard SQL Server permissions granted and revoked to these Windows logins.

For an Active Directory user to authenticate with SQL Server, a SQL Server Windows login must exist for the user or a group that the user is a member of. Fine-grained access control is handled through granting and revoking permissions on these SQL Server logins. A user that doesn't have a SQL Server login or belong to a group with such a login can't access the SQL Server DB instance.

The ALTER ANY LOGIN permission is required to create an Active Directory SQL Server login. If you haven't created any logins with this permission, connect as the DB instance's master user using SQL Server Authentication.

Run a data definition language (DDL) command such as the following example to create a SQL Server login for an Active Directory user or group.

Note

Specify users and groups using the pre-Windows 2000 login name in the format *domainName\login_name*. You can't use a user principal name (UPN) in the format *login_name@DomainName*.

```
USE [master]
GO
CREATE LOGIN [mydomain\myuser] FROM WINDOWS WITH DEFAULT_DATABASE = [master],
DEFAULT_LANGUAGE = [us_english];
GO
```

For more information, see [CREATE LOGIN \(Transact-SQL\)](#) in the Microsoft Developer Network documentation.

Users (both humans and applications) from your domain can now connect to the RDS for SQL Server instance from a domain-joined client machine using Windows authentication.

Managing a DB instance in a Domain

You can use the console, AWS CLI, or the Amazon RDS API to manage your DB instance and its relationship with your domain. For example, you can move the DB instance into, out of, or between domains.

For example, using the Amazon RDS API, you can do the following:

- To reattempt a domain join for a failed membership, use the [ModifyDBInstance](#) API operation and specify the current membership's directory ID.
- To update the IAM role name for membership, use the [ModifyDBInstance](#) API operation and specify the current membership's directory ID and the new IAM role.
- To remove a DB instance from a domain, use the [ModifyDBInstance](#) API operation and specify none as the domain parameter.
- To move a DB instance from one domain to another, use the [ModifyDBInstance](#) API operation and specify the domain identifier of the new domain as the domain parameter.
- To list membership for each DB instance, use the [DescribeDBInstances](#) API operation.

Understanding Domain membership

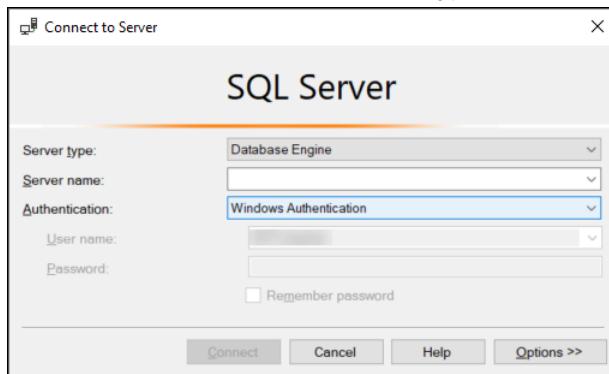
After you create or modify your DB instance, the instance becomes a member of the domain. The AWS console indicates the status of the domain membership for the DB instance. The status of the DB instance can be one of the following:

- **joined** – The instance is a member of the domain.
- **joining** – The instance is in the process of becoming a member of the domain.
- **pending-join** – The instance membership is pending.
- **pending-maintenance-join** – AWS will attempt to make the instance a member of the domain during the next scheduled maintenance window.
- **pending-removal** – The removal of the instance from the domain is pending.
- **pending-maintenance-removal** – AWS will attempt to remove the instance from the domain during the next scheduled maintenance window.
- **failed** – A configuration problem has prevented the instance from joining the domain. Check and fix your configuration before reissuing the instance modify command.
- **removing** – The instance is being removed from the domain.

A request to become a member of a domain can fail because of a network connectivity issue or an incorrect IAM role. For example, you might create a DB instance or modify an existing instance and have the attempt fail for the DB instance to become a member of a domain. In this case, either reissue the command to create or modify the DB instance or modify the newly created instance to join the domain.

Connecting to SQL Server with Windows authentication

To connect to SQL Server with Windows Authentication, you must be logged into a domain-joined computer as a domain user. After launching SQL Server Management Studio, choose **Windows Authentication** as the authentication type, as shown following.



Restoring a SQL Server DB instance and then adding it to a domain

You can restore a DB snapshot or do point-in-time recovery (PITR) for a SQL Server DB instance and then add it to a domain. Once the DB instance is restored, modify the instance using the process explained in [Step 5: Create or modify a SQL Server DB instance \(p. 1149\)](#) to add the DB instance to a domain.

Integrating an Amazon RDS for SQL Server DB instance with Amazon S3

You can transfer files between a DB instance running Amazon RDS for SQL Server and an Amazon S3 bucket. By doing this, you can use Amazon S3 with SQL Server features such as BULK INSERT. For example, you can download .csv, .xml, .txt, and other files from Amazon S3 to the DB instance host and import the data from D:\S3\ into the database. All files are stored in D:\S3\ on the DB instance.

The following limitations apply:

- Files in the D:\S3 folder are deleted on the standby replica after a failover on Multi-AZ instances. For more information, see [Multi-AZ limitations for S3 integration \(p. 1165\)](#).
- The DB instance and the S3 bucket must be in the same AWS Region.
- If you run more than one S3 integration task at a time, the tasks run sequentially, not in parallel.

Note

S3 integration tasks share the same queue as native backup and restore tasks. At maximum, you can have only two tasks in progress at any time in this queue. Therefore, two running native backup and restore tasks will block any S3 integration tasks.

- You must re-enable the S3 integration feature on restored instances. S3 integration isn't propagated from the source instance to the restored instance. Files in D:\S3 are deleted on a restored instance.
- Downloading to the DB instance is limited to 100 files. In other words, there can't be more than 100 files in D:\S3\.
- Only files without file extensions or with the following file extensions are supported for download: .abf, .asdatabase, .bcp, .configsettings, .csv, .dat, .deploymentoptions, .deploymenttargets, .fmt, .info, .isp and .xmla.
- The S3 bucket must have the same owner as the related AWS Identity and Access Management (IAM) role. Therefore, cross-account S3 integration isn't supported.
- The S3 bucket can't be open to the public.
- The file size for uploads from RDS to S3 is limited to 50 GB per file.
- The file size for downloads from S3 to RDS is limited to the maximum supported by S3.

Topics

- [Prerequisites for integrating RDS for SQL Server with S3 \(p. 1154\)](#)
- [Enabling RDS for SQL Server integration with S3 \(p. 1159\)](#)
- [Transferring files between RDS for SQL Server and Amazon S3 \(p. 1160\)](#)
- [Listing files on the RDS DB instance \(p. 1162\)](#)
- [Deleting files on the RDS DB instance \(p. 1162\)](#)
- [Monitoring the status of a file transfer task \(p. 1163\)](#)
- [Canceling a task \(p. 1165\)](#)
- [Multi-AZ limitations for S3 integration \(p. 1165\)](#)
- [Disabling RDS for SQL Server integration with S3 \(p. 1165\)](#)

For more information on working with files in Amazon S3, see [Getting started with Amazon Simple Storage Service](#).

Prerequisites for integrating RDS for SQL Server with S3

Before you begin, find or create the S3 bucket that you want to use. Also, add permissions so that the RDS DB instance can access the S3 bucket. To configure this access, you create both an IAM policy and an IAM role.

Console

To create an IAM policy for access to Amazon S3

1. In the [IAM Management Console](#), choose **Policies** in the navigation pane.
2. Create a new policy, and use the **Visual editor** tab for the following steps.
3. For **Service**, enter **S3** and then choose the **S3** service.
4. For **Actions**, choose the following to grant the access that your DB instance requires:
 - `ListAllMyBuckets` – required
 - `ListBucket` – required
 - `GetBucketACL` – required
 - `GetBucketLocation` – required
 - `GetObject` – required for downloading files from S3 to D:\S3\
 - `PutObject` – required for uploading files from D:\S3\ to S3
 - `ListMultipartUploadParts` – required for uploading files from D:\S3\ to S3
 - `AbortMultipartUpload` – required for uploading files from D:\S3\ to S3
5. For **Resources**, the options that display depend on which actions you choose in the previous step. You might see options for **bucket**, **object**, or both. For each of these, add the appropriate Amazon Resource Name (ARN).

For **bucket**, add the ARN for the bucket that you want to use. For example, if your bucket is named example-bucket, set the ARN to `arn:aws:s3:::example-bucket`.

For **object**, enter the ARN for the bucket and then choose one of the following:

- To grant access to all files in the specified bucket, choose **Any** for both **Bucket name** and **Object name**.
 - To grant access to specific files or folders in the bucket, provide ARNs for the specific buckets and objects that you want SQL Server to access.
6. Follow the instructions in the console until you finish creating the policy.

The preceding is an abbreviated guide to setting up a policy. For more detailed instructions on creating IAM policies, see [Creating IAM policies](#) in the *IAM User Guide*.

To create an IAM role that uses the IAM policy from the previous procedure

1. In the [IAM Management Console](#), choose **Roles** in the navigation pane.
2. Create a new IAM role, and choose the following options as they appear in the console:
 - **AWS service**
 - **RDS**
 - **RDS – Add Role to Database**
- Then choose **Next:Permissions** at the bottom.
3. For **Attach permissions policies**, enter the name of the IAM policy that you previously created. Then choose the policy from the list.

4. Follow the instructions in the console until you finish creating the role.

The preceding is an abbreviated guide to setting up a role. If you want more detailed instructions on creating roles, see [IAM roles](#) in the *IAM User Guide*.

AWS CLI

To grant Amazon RDS access to an Amazon S3 bucket, use the following process:

1. Create an IAM policy that grants Amazon RDS access to an S3 bucket.
2. Create an IAM role that Amazon RDS can assume on your behalf to access your S3 buckets.

For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

3. Attach the IAM policy that you created to the IAM role that you created.

To create the IAM policy

Include the appropriate actions to grant the access your DB instance requires:

- `ListAllMyBuckets` – required
- `ListBucket` – required
- `GetBucketACL` – required
- `GetBucketLocation` – required
- `GetObject` – required for downloading files from S3 to D:\S3\
- `PutObject` – required for uploading files from D:\S3\ to S3
- `ListMultipartUploadParts` – required for uploading files from D:\S3\ to S3
- `AbortMultipartUpload` – required for uploading files from D:\S3\ to S3

1. The following AWS CLI command creates an IAM policy named `rds-s3-integration-policy` with these options. It grants access to a bucket named `bucket_name`.

Example

For Linux, macOS, or Unix:

```
aws iam create-policy \
--policy-name rds-s3-integration-policy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3>ListBucket",
                "s3>GetBucketACL",
                "s3>GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::bucket_name"
        }
    ]
}'
```

```
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3>ListMultipartUploadParts",
            "s3:AbortMultipartUpload"
        ],
        "Resource": "arn:aws:s3:::bucket_name/key_prefix/*"
    }
]
}'
```

For Windows:

Make sure to change the line endings to the ones supported by your interface (^ instead of \). Also, in Windows, you must escape all double quotes with a \. To avoid the need to escape the quotes in the JSON, you can save it to a file instead and pass that in as a parameter.

First, create the `policy.json` file with the following permission policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3>ListBucket",
                "s3:GetBucketACL",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::bucket_name"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3>ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::bucket_name/key_prefix/*"
        }
    ]
}
```

Then use the following command to create the policy:

```
aws iam create-policy ^
--policy-name rds-s3-integration-policy ^
--policy-document file://file_path/assume_role_policy.json
```

2. After the policy is created, note the Amazon Resource Name (ARN) of the policy. You need the ARN for a later step.

To create the IAM role

- The following AWS CLI command creates the `rds-s3-integration-role` IAM role for this purpose.

Example

For Linux, macOS, or Unix:

```
aws iam create-role \
--role-name rds-s3-integration-role \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}'
```

For Windows:

Make sure to change the line endings to the ones supported by your interface (^ instead of \). Also, in Windows, you must escape all double quotes with a \. To avoid the need to escape the quotes in the JSON, you can save it to a file instead and pass that in as a parameter.

First, create the `assume_role_policy.json` file with the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rds.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Then use the following command to create the IAM role:

```
aws iam create-role ^
--role-name rds-s3-integration-role ^
--assume-role-policy-document file://file_path/assume_role_policy.json
```

Example of using the global condition context key to create the IAM role

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based policies to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the policy, make sure to use the `aws:SourceArn` global condition context key with the full Amazon Resource Name (ARN) of the resources accessing the role. For S3 integration, make sure to include the DB instance ARNs, as shown in the following example.

For Linux, macOS, or Unix:

```
aws iam create-role \
    --role-name rds-s3-integration-role \
    --assume-role-policy-document '{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {
                    "Service": "rds.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
                "Condition": {
                    "StringEquals": {
                        "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                    }
                }
            }
        ]
    }'
```

For Windows:

Add the global condition context key to `assume_role_policy.json`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rds.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                }
            }
        }
    ]
}
```

To attach the IAM policy to the IAM role

- The following AWS CLI command attaches the policy to the role named `rds-s3-integration-role`. Replace `your-policy-arn` with the policy ARN that you noted in a previous step.

Example

For Linux, macOS, or Unix:

```
aws iam attach-role-policy \
--policy-arn your-policy-arn \
--role-name rds-s3-integration-role
```

For Windows:

```
aws iam attach-role-policy ^
--policy-arn your-policy-arn ^
--role-name rds-s3-integration-role
```

Enabling RDS for SQL Server integration with S3

In the following section, you can find how to enable Amazon S3 integration with Amazon RDS for SQL Server. To work with S3 integration, your DB instance must be associated with the IAM role that you previously created before you use the `S3_INTEGRATION` feature-name parameter.

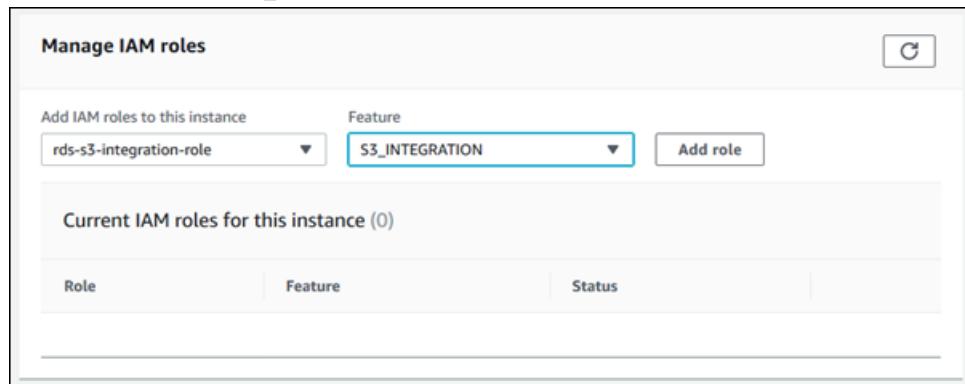
Note

To add an IAM role to a DB instance, the status of the DB instance must be **available**.

Console

To associate your IAM role with your DB instance

- Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
- Choose the RDS for SQL Server DB instance name to display its details.
- On the **Connectivity & security** tab, in the **Manage IAM roles** section, choose the IAM role to add for **Add IAM roles to this instance**.
- For **Feature**, choose `S3_INTEGRATION`.



- Choose **Add role**.

AWS CLI

To add the IAM role to the RDS for SQL Server DB instance

- The following AWS CLI command adds your IAM role to an RDS for SQL Server DB instance named *mydbinstance*.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-instance \
--db-instance-identifier mydbinstance \
--feature-name S3_INTEGRATION \
--role-arn your-role-arn
```

For Windows:

```
aws rds add-role-to-db-instance ^
--db-instance-identifier mydbinstance ^
--feature-name S3_INTEGRATION ^
--role-arn your-role-arn
```

Replace *your-role-arn* with the role ARN that you noted in a previous step. S3_INTEGRATION must be specified for the --feature-name option.

Transferring files between RDS for SQL Server and Amazon S3

You can use Amazon RDS stored procedures to download and upload files between Amazon S3 and your RDS DB instance. You can also use Amazon RDS stored procedures to list and delete files on the RDS instance.

The files that you download from and upload to S3 are stored in the D:\S3 folder. This is the only folder that you can use to access your files. You can organize your files into subfolders, which are created for you when you include the destination folder during download.

Some of the stored procedures require that you provide an Amazon Resource Name (ARN) to your S3 bucket and file. The format for your ARN is `arn:aws:s3:::bucket_name/file_name`. Amazon S3 doesn't require an account number or AWS Region in ARNs.

S3 integration tasks run sequentially and share the same queue as native backup and restore tasks. At maximum, you can have only two tasks in progress at any time in this queue. It can take up to five minutes for the task to begin processing.

Downloading files from an Amazon S3 bucket to a SQL Server DB instance

To download files from an S3 bucket to an RDS for SQL Server DB instance, use the Amazon RDS stored procedure `msdb.dbo.rds_download_from_s3` with the following parameters.

Parameter name	Data type	Default	Required	Description
<code>@s3_arn_of_file</code>	NVARCHAR	-	Required	The S3 ARN of the file to download, for example: <code>arn:aws:s3:::bucket_name/mydata.csv</code>

Parameter name	Data type	Default	Required	Description
@rds_file_path	NVARCHAR	–	Optional	The file path for the RDS instance. If not specified, the file path is D:\S3\<filename in s3>. RDS supports absolute paths and relative paths. If you want to create a subfolder, include it in the file path.
@overwrite_file	INT	0	Optional	Overwrite the existing file: 0 = Don't overwrite 1 = Overwrite

You can download files without a file extension and files with the following file extensions: .bcf, .csv, .dat, .fmt, .info, .lst, .tbl, .txt, and .xml.

Note

Files with the .ispac file extension are supported for download when SQL Server Integration Services is enabled. For more information on enabling SSIS, see [SQL Server Integration Services \(p. 1251\)](#).

Files with the following file extensions are supported for download when SQL Server Analysis Services is enabled: .abf, .asdatabase, .configsettings, .deploymentoptions, .deploymenttargets, and .xmla. For more information on enabling SSAS, see [SQL Server Analysis Services \(p. 1232\)](#).

The following example shows the stored procedure to download files from S3.

```
exec msdb.dbo.rds_download_from_s3
    @s3_arn_of_file='arn:aws:s3:::bucket_name/bulk_data.csv',
    @rds_file_path='D:\S3\seed_data\data.csv',
    @overwrite_file=1;
```

The example rds_download_from_s3 operation creates a folder named seed_data in D:\S3\, if the folder doesn't exist yet. Then the example downloads the source file bulk_data.csv from S3 to a new file named data.csv on the DB instance. If the file previously existed, it's overwritten because the @overwrite_file parameter is set to 1.

Uploading files from a SQL Server DB instance to an Amazon S3 bucket

To upload files from an RDS for SQL Server DB instance to an S3 bucket, use the Amazon RDS stored procedure msdb.dbo.rds_upload_to_s3 with the following parameters.

Parameter name	Data type	Default	Required	Description
@s3_arn_of_file	NVARCHAR	–	Required	The S3 ARN of the file to be created in S3, for example: arn:aws:s3:::bucket_name/mydata.csv
@rds_file_path	NVARCHAR	–	Required	The file path of the file to upload to S3. Absolute and relative paths are supported.

Parameter name	Data type	Default	Required	Description
@overwrite_file	INT	–	Optional	Overwrite the existing file: 0 = Don't overwrite 1 = Overwrite

The following example uploads the file named `data.csv` from the specified location in `D:\S3\seed_data\` to a file `new_data.csv` in the S3 bucket specified by the ARN.

```
exec msdb.dbo.rds_upload_to_s3
    @rds_file_path='D:\S3\seed_data\data.csv',
    @s3_arn_of_file='arn:aws:s3:::bucket_name/new_data.csv',
    @overwrite_file=1;
```

If the file previously existed in S3, it's overwritten because the `@overwrite_file` parameter is set to 1.

Listing files on the RDS DB instance

To list the files available on the DB instance, use both a stored procedure and a function. First, run the following stored procedure to gather file details from the files in `D:\S3\`.

```
exec msdb.dbo.rds_gather_file_details;
```

The stored procedure returns the ID of the task. Like other tasks, this stored procedure runs asynchronously. As soon as the status of the task is `SUCCESS`, you can use the task ID in the `rds_fn_list_file_details` function to list the existing files and directories in `D:\S3\`, as shown following.

```
SELECT * FROM msdb.dbo.rds_fn_list_file_details(TASK_ID);
```

The `rds_fn_list_file_details` function returns a table with the following columns.

Output parameter	Description
<code>filepath</code>	Absolute path of the file (for example, <code>D:\S3\mydata.csv</code>)
<code>size_in_bytes</code>	File size (in bytes)
<code>last_modified_utc</code>	Last modification date and time in UTC format
<code>is_directory</code>	Option that indicates whether the item is a directory (true/false)

Deleting files on the RDS DB instance

To delete the files available on the DB instance, use the Amazon RDS stored procedure `msdb.dbo.rds_delete_from_filesystem` with the following parameters.

Parameter name	Data type	Default	Required	Description
@rds_file_path	NVARCHAR	–	Required	The file path of the file to delete. Absolute and relative paths are supported.
@force_delete	INT	0	Optional	To delete a directory, this flag must be included and set to 1. 1 = delete a directory This parameter is ignored if you are deleting a file.

To delete a directory, the @rds_file_path must end with a backslash (\) and @force_delete must be set to 1.

The following example deletes the file D:\S3\delete_me.txt.

```
exec msdb.dbo.rds_delete_from_filesystem
    @rds_file_path='D:\S3\delete_me.txt';
```

The following example deletes the directory D:\S3\example_folder\.

```
exec msdb.dbo.rds_delete_from_filesystem
    @rds_file_path='D:\S3\example_folder\' ,
    @force_delete=1;
```

Monitoring the status of a file transfer task

To track the status of your S3 integration task, call the rds_fn_task_status function. It takes two parameters. The first parameter should always be NULL because it doesn't apply to S3 integration. The second parameter accepts a task ID.

To see a list of all tasks, set the first parameter to NULL and the second parameter to 0, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

To get a specific task, set the first parameter to NULL and the second parameter to the task ID, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

The rds_fn_task_status function returns the following information.

Output parameter	Description
task_id	The ID of the task.
task_type	For S3 integration, tasks can have the following task types:

Output parameter	Description
	<ul style="list-style-type: none"> • DOWNLOAD_FROM_S3 • UPLOAD_TO_S3 • LIST_FILES_ON_DISK • DELETE_FILES_ON_DISK
database_name	Not applicable to S3 integration tasks.
% complete	The progress of the task as a percentage.
duration(mins)	The amount of time spent on the task, in minutes.
lifecycle	<p>The status of the task. Possible statuses are the following:</p> <ul style="list-style-type: none"> • CREATED – After you call one of the S3 integration stored procedures, a task is created and the status is set to CREATED. • IN_PROGRESS – After a task starts, the status is set to IN_PROGRESS. It can take up to five minutes for the status to change from CREATED to IN_PROGRESS. • SUCCESS – After a task completes, the status is set to SUCCESS. • ERROR – If a task fails, the status is set to ERROR. For more information about the error, see the task_info column. • CANCEL_REQUESTED – After you call rds_cancel_task, the status of the task is set to CANCEL_REQUESTED. • CANCELLED – After a task is successfully canceled, the status of the task is set to CANCELLED.
task_info	Additional information about the task. If an error occurs during processing, this column contains information about the error.
last_updated	The date and time that the task status was last updated.
created_at	The date and time that the task was created.
S3_object_arn	The ARN of the S3 object downloaded from or uploaded to.
overwrite_S3_backup_file	Not applicable to S3 integration tasks.
KMS_master_key_arn	Not applicable to S3 integration tasks.
filepath	The file path on the RDS DB instance.
overwrite_file	An option that indicates if an existing file is overwritten.
task_metadata	Not applicable to S3 integration tasks.

Cancelling a task

To cancel S3 integration tasks, use the `msdb.dbo.rds_cancel_task` stored procedure with the `task_id` parameter. Delete and list tasks that are in progress can't be cancelled. The following example shows a request to cancel a task.

```
exec msdb.dbo.rds_cancel_task @task_id = 1234;
```

To get an overview of all tasks and their task IDs, use the `rds_fn_task_status` function as described in [Monitoring the status of a file transfer task \(p. 1163\)](#).

Multi-AZ limitations for S3 integration

On Multi-AZ instances, files in the `D:\S3` folder are deleted on the standby replica after a failover. A failover can be planned, for example, during DB instance modifications such as changing the instance class or upgrading the engine version. Or a failover can be unplanned, during an outage of the primary.

Note

We don't recommend using the `D:\S3` folder for file storage. The best practice is to upload created files to Amazon S3 to make them durable, and download files when you need to import data.

To determine the last failover time, you can use the `msdb.dbo.rds_failover_time` stored procedure. For more information, see [Determining the last failover time \(p. 1300\)](#).

Example of no recent failover

This example shows the output when there is no recent failover in the error logs. No failover has happened since 2020-04-29 23:59:00.01.

Therefore, all files downloaded after that time that haven't been deleted using the `rds_delete_from_filesystem` stored procedure are still accessible on the current host. Files downloaded before that time might also be available.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example of recent failover

This example shows the output when there is a failover in the error logs. The most recent failover was at 2020-05-05 18:57:51.89.

All files downloaded after that time that haven't been deleted using the `rds_delete_from_filesystem` stored procedure are still accessible on the current host.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Disabling RDS for SQL Server integration with S3

Following, you can find how to disable Amazon S3 integration with Amazon RDS for SQL Server. Files in `D:\S3\` aren't deleted when disabling S3 integration.

Note

To remove an IAM role from a DB instance, the status of the DB instance must be available.

Console

To disassociate your IAM role from your DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose the RDS for SQL Server DB instance name to display its details.
3. On the **Connectivity & security** tab, in the **Manage IAM roles** section, choose the IAM role to remove.
4. Choose **Delete**.

AWS CLI

To remove the IAM role from the RDS for SQL Server DB instance

- The following AWS CLI command removes the IAM role from a RDS for SQL Server DB instance named *mydbinstance*.

Example

For Linux, macOS, or Unix:

```
aws rds remove-role-from-db-instance \
    --db-instance-identifier mydbinstance \
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

For Windows:

```
aws rds remove-role-from-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

Replace *your-role-arn* with the appropriate IAM role ARN for the --feature-name option.

Using Database Mail on Amazon RDS for SQL Server

You can use Database Mail to send email messages to users from your Amazon RDS on SQL Server database instance. The messages can contain files and query results. Database Mail includes the following components:

- **Configuration and security objects** – These objects create profiles and accounts, and are stored in the msdb database.
- **Messaging objects** – These objects include the `sp_send_dbmail` stored procedure used to send messages, and data structures that hold information about messages. They're stored in the msdb database.
- **Logging and auditing objects** – Database Mail writes logging information to the msdb database and the Microsoft Windows application event log.
- **Database Mail executable** – `DatabaseMail.exe` reads from a queue in the msdb database and sends email messages.

RDS supports Database Mail for all SQL Server versions on the Web, Standard, and Enterprise Editions.

Limitations

The following limitations apply to using Database Mail on your SQL Server DB instance:

- Database Mail isn't supported for SQL Server Express Edition.
- Modifying Database Mail configuration parameters isn't supported. To see the preset (default) values, use the `sysmail_help_configure_sp` stored procedure.
- File attachments aren't fully supported. For more information, see [Working with file attachments \(p. 1176\)](#).
- The maximum file attachment size is 1 MB.
- Database Mail requires additional configuration on Multi-AZ DB instances. For more information, see [Considerations for Multi-AZ deployments \(p. 1177\)](#).
- Configuring SQL Server Agent to send email messages to predefined operators isn't supported.

Enabling Database Mail

Use the following process to enable Database Mail for your DB instance:

1. Create a new parameter group.
2. Modify the parameter group to set the `database mail xps` parameter to 1.
3. Associate the parameter group with the DB instance.

Creating the parameter group for Database Mail

Create a parameter group for the `database mail xps` parameter that corresponds to the SQL Server edition and version of your DB instance.

Note

You can also modify an existing parameter group. Follow the procedure in [Modifying the parameter that enables Database Mail \(p. 1168\)](#).

Console

The following example creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.
4. In the **Create parameter group** pane, do the following:
 - a. For **Parameter group family**, choose **sqlserver-se-13.0**.
 - b. For **Group name**, enter an identifier for the parameter group, such as **dbmail-sqlserver-se-13**.
 - c. For **Description**, enter **Database Mail XPs**.
5. Choose **Create**.

CLI

The following example creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
--db-parameter-group-name dbmail-sqlserver-se-13 \
--db-parameter-group-family "sqlserver-se-13.0" \
--description "Database Mail XPs"
```

For Windows:

```
aws rds create-db-parameter-group ^
--db-parameter-group-name dbmail-sqlserver-se-13 ^
--db-parameter-group-family "sqlserver-se-13.0" ^
--description "Database Mail XPs"
```

Modifying the parameter that enables Database Mail

Modify the `database mail xps` parameter in the parameter group that corresponds to the SQL Server edition and version of your DB instance.

To enable Database Mail, set the `database mail xps` parameter to 1.

Console

The following example modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.

3. Choose the parameter group, such as **dbmail-sqlserver-se-13**.
4. Under **Parameters**, filter the parameter list for **mail**.
5. Choose **database mail xps**.
6. Choose **Edit parameters**.
7. Enter **1**.
8. Choose **Save changes**.

CLI

The following example modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name dbmail-sqlserver-se-13 \
--parameters "ParameterName='database mail
xps',ParameterValue=1,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name dbmail-sqlserver-se-13 ^
--parameters "ParameterName='database mail
xps',ParameterValue=1,ApplyMethod=immediate"
```

Associating the parameter group with the DB instance

You can use the AWS Management Console or the AWS CLI to associate the Database Mail parameter group with the DB instance.

Console

You can associate the Database Mail parameter group with a new or existing DB instance.

- For a new DB instance, associate it when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, associate it by modifying the instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

You can associate the Database Mail parameter group with a new or existing DB instance.

To create a DB instance with the Database Mail parameter group

- Specify the same DB engine type and major version as you used when creating the parameter group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier mydbinstance \
--db-instance-class db.m5.2xlarge \
--engine sqlserver-se \
--engine-version 13.00.5426.0.v1 \
--allocated-storage 100 \
--master-user-password secret123 \
--master-username admin \
--storage-type gp2 \
--license-model li \
--db-parameter-group-name dbmail-sqlserver-se-13
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--db-instance-class db.m5.2xlarge ^
--engine sqlserver-se ^
--engine-version 13.00.5426.0.v1 ^
--allocated-storage 100 ^
--master-user-password secret123 ^
--master-username admin ^
--storage-type gp2 ^
--license-model li ^
--db-parameter-group-name dbmail-sqlserver-se-13
```

To modify a DB instance and associate the Database Mail parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--db-parameter-group-name dbmail-sqlserver-se-13 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--db-parameter-group-name dbmail-sqlserver-se-13 ^
--apply-immediately
```

Configuring Database Mail

You perform the following tasks to configure Database Mail:

1. Create the Database Mail profile.

2. Create the Database Mail account.
3. Add the Database Mail account to the Database Mail profile.
4. Add users to the Database Mail profile.

Note

To configure Database Mail, make sure that you have execute permission on the stored procedures in the msdb database.

Creating the Database Mail profile

To create the Database Mail profile, you use the [sysmail_add_profile_sp](#) stored procedure. The following example creates a profile named Notifications.

To create the profile

- Use the following SQL statement.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_profile_sp
    @profile_name      = 'Notifications',
    @description       = 'Profile used for sending outgoing notifications using
                        Amazon SES.';
GO
```

Creating the Database Mail account

To create the Database Mail account, you use the [sysmail_add_account_sp](#) stored procedure. The following example creates an account named SES that uses Amazon Simple Email Service.

Using Amazon SES requires the following parameters:

- `@email_address` – An Amazon SES verified identity. For more information, see [Verified identities in Amazon SES](#).
- `@mailserver_name` – An Amazon SES SMTP endpoint. For more information, see [Connecting to an Amazon SES SMTP endpoint](#).
- `@username` – An Amazon SES SMTP user name. For more information, see [Obtaining Amazon SES SMTP credentials](#).

Don't use an AWS Identity and Access Management user name.

- `@password` – An Amazon SES SMTP password. For more information, see [Obtaining Amazon SES SMTP credentials](#).

To create the account

- Use the following SQL statement.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_account_sp
    @account_name      = 'SES',
    @description       = 'Mail account for sending outgoing notifications.',
```

```
@email_address      = 'nobody@example.com',
@email_display_name = 'Automated Mailer',
@mailserver_name    = 'email-smtp.us-west-2.amazonaws.com',
@port               = 587,
@Enable_Ssl          = 1,
@username            = 'Smtip_Username',
@password            = 'Smtip_Password';
GO
```

Adding the Database Mail account to the Database Mail profile

To add the Database Mail account to the Database Mail profile, you use the [sysmail_add_profileaccount_sp](#) stored procedure. The following example adds the SES account to the Notifications profile.

To add the account to the profile

- Use the following SQL statement.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_profileaccount_sp
    @profile_name      = 'Notifications',
    @account_name       = 'SES',
    @sequence_number    = 1;
GO
```

Adding users to the Database Mail profile

To grant permission for an msdb database principal to use a Database Mail profile, you use the [sysmail_add_principalprofile_sp](#) stored procedure. A *principal* is an entity that can request SQL Server resources. The database principal must map to a SQL Server authentication user, a Windows Authentication user, or a Windows Authentication group.

The following example grants public access to the Notifications profile.

To add a user to the profile

- Use the following SQL statement.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_principalprofile_sp
    @profile_name      = 'Notifications',
    @principal_name     = 'public',
    @is_default         = 1;
GO
```

Amazon RDS stored procedures and functions for Database Mail

Microsoft provides [stored procedures](#) for using Database Mail, such as creating, listing, updating, and deleting accounts and profiles. In addition, RDS provides the stored procedures and functions for Database Mail shown in the following table.

Procedure/Function	Description
rds_fn_sysmail_allitems	Shows sent messages, including those submitted by other users.
rds_fn_sysmail_event_log	Shows events, including those for messages submitted by other users.
rds_fn_sysmail_mailattachments	Shows attachments, including those to messages submitted by other users.
rds_sysmail_control	Starts and stops the mail queue (DatabaseMail.exe process).
rds_sysmail_delete_mailitems_sp	Deletes email messages sent by all users from the Database Mail internal tables.

Sending email messages using Database Mail

You use the `sp_send_dbmail` stored procedure to send email messages using Database Mail.

Usage

```
EXEC msdb.dbo.sp_send_dbmail
@profile_name = 'profile_name',
@recipients = 'recipient1@example.com[; recipient2; ... recipientn]',
@subject = 'subject',
@body = 'message_body',
[@body_format = 'HTML'],
[@file_attachments = 'file_path1; file_path2; ... file_pathn'],
[@query = 'SQL_query'],
[@attach_query_result_as_file = 0/1];
```

The following parameters are required:

- `@profile_name` – The name of the Database Mail profile from which to send the message.
- `@recipients` – The semicolon-delimited list of email addresses to which to send the message.
- `@subject` – The subject of the message.
- `@body` – The body of the message. You can also use a declared variable as the body.

The following parameters are optional:

- `@body_format` – This parameter is used with a declared variable to send email in HTML format.
- `@file_attachments` – The semicolon-delimited list of message attachments. File paths must be absolute paths.
- `@query` – A SQL query to run. The query results can be attached as a file or included in the body of the message.
- `@attach_query_result_as_file` – Whether to attach the query result as a file. Set to 0 for no, 1 for yes. The default is 0.

Examples

The following examples demonstrate how to send email messages.

Example of sending a message to a single recipient

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
    @profile_name      = 'Notifications',
    @recipients        = 'nobody@example.com',
    @subject           = 'Automated DBMail message - 1',
    @body               = 'Database Mail configuration was successful.';
GO
```

Example of sending a message to multiple recipients

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
    @profile_name      = 'Notifications',
    @recipients         = 'recipient1@example.com;recipient2@example.com',
    @subject            = 'Automated DBMail message - 2',
    @body                = 'This is a message.';
GO
```

Example of sending a SQL query result as a file attachment

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
    @profile_name      = 'Notifications',
    @recipients         = 'nobody@example.com',
    @subject            = 'Test SQL query',
    @body                = 'This is a SQL query test.',
    @query               = 'SELECT * FROM abc.dbo.test',
    @attach_query_result_as_file = 1;
GO
```

Example of sending a message in HTML format

```
USE msdb
GO

DECLARE @HTML_Body as NVARCHAR(500) = 'Hi, <h4> Heading </h4> <br> See the report. <b>
Regards </b>';
EXEC msdb.dbo.sp_send_dbmail
    @profile_name      = 'Notifications',
    @recipients         = 'nobody@example.com',
    @subject            = 'Test HTML message',
    @body                = @HTML_Body,
    @body_format        = 'HTML';
GO
```

Example of sending a message using a trigger when a specific event occurs in the database

```
USE AdventureWorks2017
GO
IF OBJECT_ID ('Production.iProductNotification', 'TR') IS NOT NULL
DROP TRIGGER Purchasing.iProductNotification
```

```
GO

CREATE TRIGGER iProductNotification ON Production.Product
FOR INSERT
AS
DECLARE @ProductInformation nvarchar(255);
SELECT
@ProductInformation = 'A new product, ' + Name + ', is now available for $' +
CAST(StandardCost AS nvarchar(20)) + '!'
FROM INSERTED i;

EXEC msdb.dbo.sp_send_dbmail
@profile_name      = 'Notifications',
@recipients        = 'nobody@example.com',
@subject           = 'New product information',
@body               = @ProductInformation;
GO
```

Viewing messages, logs, and attachments

You use RDS stored procedures to view messages, event logs, and attachments.

To view all email messages

- Use the following SQL query.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_allitems(); --WHERE sent_status='sent' or
'failed' or 'unsent'
```

To view all email event logs

- Use the following SQL query.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_event_log();
```

To view all email attachments

- Use the following SQL query.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_mailattachments();
```

Deleting messages

You use the `rds_sysmail_delete_mailitems_sp` stored procedure to delete messages.

Note

RDS automatically deletes mail table items when DBMail history data reaches 1 GB in size, with a retention period of at least 24 hours.

If you want to keep mail items for a longer period, you can archive them. For more information, see [Create a SQL Server Agent job to archive Database Mail messages and event logs](#) in the Microsoft documentation.

To delete all email messages

- Use the following SQL statement.

```
DECLARE @GETDATE datetime
SET @GETDATE = GETDATE();
EXECUTE msdb.dbo.rds_sysmail_delete_mailitems_sp @sent_before = @GETDATE;
GO
```

To delete all email messages with a particular status

- Use the following SQL statement to delete all failed messages.

```
DECLARE @GETDATE datetime
SET @GETDATE = GETDATE();
EXECUTE msdb.dbo.rds_sysmail_delete_mailitems_sp @sent_status = 'failed';
GO
```

Starting the mail queue

You use the `rds_sysmail_control` stored procedure to start the Database Mail process.

Note

Enabling Database Mail automatically starts the mail queue.

To start the mail queue

- Use the following SQL statement.

```
EXECUTE msdb.dbo.rds_sysmail_control start;
GO
```

Stopping the mail queue

You use the `rds_sysmail_control` stored procedure to stop the Database Mail process.

To stop the mail queue

- Use the following SQL statement.

```
EXECUTE msdb.dbo.rds_sysmail_control stop;
GO
```

Working with file attachments

The following file attachment extensions aren't supported in Database Mail messages from RDS on SQL Server: .ade, .adp, .apk, .appx, .appxbundle, .bat, .bak, .cab, .chm, .cmd, .com, .cpl, .dll, .dmg, .exe, .hta, .inf1, .ins, .isp, .isw, and .wsh.

Database Mail uses the Microsoft Windows security context of the current user to control access to files. Users who log in with SQL Server Authentication can't attach files using the `@file_attachments` parameter with the `sp_send_dbmail` stored procedure. Windows doesn't allow SQL Server to provide credentials from a remote computer to another remote computer. Therefore, Database Mail can't attach files from a network share when the command is run from a computer other than the computer running SQL Server.

However, you can use SQL Server Agent jobs to attach files. For more information on SQL Server Agent, see [Using SQL Server Agent \(p. 1305\)](#) and [SQL Server Agent](#) in the Microsoft documentation.

Considerations for Multi-AZ deployments

When you configure Database Mail on a Multi-AZ DB instance, the configuration isn't automatically propagated to the secondary. We recommend converting the Multi-AZ instance to a Single-AZ instance, configuring Database Mail, and then converting the DB instance back to Multi-AZ. Then both the primary and secondary nodes have the Database Mail configuration.

If you create a read replica from your Multi-AZ instance that has Database Mail configured, the replica inherits the configuration, but without the password to the SMTP server. Update the Database Mail account with the password.

Instance store support for the tempdb database on Amazon RDS for SQL Server

An *instance store* provides temporary block-level storage for your DB instance. This storage is located on disks that are physically attached to the host computer. These disks have Non-Volatile Memory Express (NVMe) instance storage that is based on solid-state drives (SSDs). This storage is optimized for low latency, very high random I/O performance, and high sequential read throughput.

By placing tempdb data files and tempdb log files on the instance store, you can achieve lower read and write latencies compared to standard storage based on Amazon EBS.

Note

SQL Server database files and database log files aren't placed on the instance store.

Enabling the instance store

When RDS provisions DB instances with one of the following instance classes, the tempdb database is automatically placed onto the instance store:

- db.m5d
- db.r5d

To enable the instance store, do one of the following:

- Create a SQL Server DB instance using one of these instance types. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- Modify an existing SQL Server DB instance to use one of them. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

The instance store is available in all AWS Regions where one or more of these instance types are supported. For more information on the db.m5d and db.r5d instance classes, see [DB instance classes \(p. 10\)](#). For more information on the instance classes supported by Amazon RDS for SQL Server, see [DB instance class support for Microsoft SQL Server \(p. 1062\)](#).

File location and size considerations

On instances without an instance store, RDS stores the tempdb data and log files in the D:\rdsdbdata\DATA directory. Both files start at 8 MB by default.

On instances with an instance store, RDS stores the tempdb data and log files in the T:\rdsdbdata\DATA directory.

When tempdb has only one data file (tempdb.mdf) and one log file (templog.ldf), templog.ldf starts at 8 MB by default and tempdb.mdf starts at 80% or more of the instance's storage capacity. Twenty percent of the storage capacity or 200 GB, whichever is less, is kept free to start. Multiple tempdb data files split the 80% disk space evenly, while log files always have an 8-MB initial size.

For example, if you modify your DB instance class from db.m5.2xlarge to db.m5d.2xlarge, the size of tempdb data files increases from 8 MB each to 234 GB in total.

Note

Besides the tempdb data and log files on the instance store (T:\rdsdbdata\DATA), you can still create extra tempdb data and log files on the data volume (D:\rdsdbdata\DATA). Those files always have an 8 MB initial size.

Backup considerations

You might need to retain backups for long periods, incurring costs over time. The tempdb data and log blocks can change very often depending on the workload. This can greatly increase the DB snapshot size.

When tempdb is on the instance store, snapshots don't include temporary files. This means that snapshot sizes are smaller and consume less of the free backup allocation compared to EBS-only storage.

Disk full errors

If you use all of the available space in the instance store, you might receive errors such as the following:

- The transaction log for database 'tempdb' is full due to 'ACTIVE_TRANSACTION'.
- Could not allocate space for object 'dbo.SORT temporary run storage: 140738941419520' in database 'tempdb' because the 'PRIMARY' filegroup is full. Create disk space by deleting unneeded files, dropping objects in the filegroup, adding additional files to the filegroup, or setting autogrowth on for existing files in the filegroup.

You can do one or more of the following when the instance store is full:

- Adjust your workload or the way you use tempdb.
- Scale up to use a DB instance class with more NVMe storage.
- Stop using the instance store, and use an instance class with only EBS storage.
- Use a mixed mode by adding secondary data or log files for tempdb on the EBS volume.

Removing the instance store

To remove the instance store, modify your SQL Server DB instance to use an instance type that doesn't support instance store, such as db.m5 or db.r5.

Note

When you remove the instance store, the temporary files are moved to the D:\rdsdbdata\DATA directory and reduced in size to 8 MB.

Using extended events with Amazon RDS for Microsoft SQL Server

You can use extended events in Microsoft SQL Server to capture debugging and troubleshooting information for Amazon RDS for SQL Server. Extended events replace SQL Trace and Server Profiler, which have been deprecated by Microsoft. Extended events are similar to profiler traces but with more granular control on the events being traced. Extended events are supported for SQL Server versions 2014 and later on Amazon RDS. For more information, see [Extended events overview](#) in the Microsoft documentation.

Extended events are turned on automatically for users with master user privileges in Amazon RDS for SQL Server.

Topics

- [Limitations and recommendations \(p. 1180\)](#)
- [Configuring extended events on RDS for SQL Server \(p. 1180\)](#)
- [Considerations for Multi-AZ deployments \(p. 1181\)](#)
- [Querying extended event files \(p. 1182\)](#)

Limitations and recommendations

When using extended events on RDS for SQL Server, the following limitations apply:

- Extended events are supported only for the Enterprise and Standard Editions.
- You can't alter default extended event sessions.
- Make sure to set the session memory partition mode to NONE.
- Session event retention mode can be either ALLOW_SINGLE_EVENT_LOSS or ALLOW_MULTIPLE_EVENT_LOSS.
- Event Tracing for Windows (ETW) targets aren't supported.
- Make sure that file targets are in the D:\rdsdbdata\log directory.
- For pair matching targets, set the respond_to_memory_pressure property to 1.
- Ring buffer target memory can't be greater than 4 MB.
- The following actions aren't supported:
 - debug_break
 - create_dump_all_threads
 - create_dump_single_threads
- The rpc_completed event is supported on the following versions and later: 15.0.4083.2, 14.0.3370.1, 13.0.5865.1, 12.0.6433.1, 11.0.7507.2.

Configuring extended events on RDS for SQL Server

On RDS for SQL Server, you can configure the values of certain parameters of extended event sessions. The following table describes the configurable parameters.

Parameter name	Description
xe_session_max_memory	Specifies the maximum amount
xe_session_max_event_size	Specifies the maximum memory

Parameter name	Description
xe_session_max_dispatch_latency	Specifies the amount of time that the event session.
xe_file_target_size	Specifies the maximum size of the .xel file.
xe_file_retention	Specifies the retention time in days.

Note

Setting `xe_file_retention` to zero causes .xel files to be removed automatically after the lock on these files is released by SQL Server. The lock is released whenever an .xel file reaches the size limit set in `xe_file_target_size`.

You can use the `rdsadmin.dbo.rds_show_configuration` stored procedure to show the current values of these parameters. For example, use the following SQL statement to view the current setting of `xe_session_max_memory`.

```
exec rdsadmin..rds_show_configuration 'xe_session_max_memory'
```

You can use the `rdsadmin.dbo.rds_set_configuration` stored procedure to modify them. For example, use the following SQL statement to set `xe_session_max_memory` to 4 MB.

```
exec rdsadmin..rds_set_configuration 'xe_session_max_memory', 4
```

Considerations for Multi-AZ deployments

When you create an extended event session on a primary DB instance, it doesn't propagate to the standby replica. You can fail over and create the extended event session on the new primary DB instance. Or you can remove and then re-add the Multi-AZ configuration to propagate the extended event session to the standby replica. RDS stops all nondefault extended event sessions on the standby replica, so that these sessions don't consume resources on the standby. Because of this, after a standby replica becomes the primary DB instance, make sure to manually start the extended event sessions on the new primary.

Note

This approach applies to both Always On Availability Groups and Database Mirroring.

You can also use a SQL Server Agent job to track the standby replica and start the sessions if the standby becomes the primary. For example, use the following query in your SQL Server Agent job step to restart event sessions on a primary DB instance.

```
BEGIN
    IF (DATABASEPROPERTYEX('rdsadmin','Updateability')='READ_WRITE'
        AND DATABASEPROPERTYEX('rdsadmin','status')='ONLINE'
        AND (DATABASEPROPERTYEX('rdsadmin','Collation') IS NOT NULL OR
        DATABASEPROPERTYEX('rdsadmin','IsAutoClose')=1)
    )
    BEGIN
        IF NOT EXISTS (SELECT 1 FROM sys.dm_xe_sessions WHERE name='xe1')
            ALTER EVENT SESSION xe1 ON SERVER STATE=START
        IF NOT EXISTS (SELECT 1 FROM sys.dm_xe_sessions WHERE name='xe2')
            ALTER EVENT SESSION xe2 ON SERVER STATE=START
    END
END
```

This query restarts the event sessions `xe1` and `xe2` on a primary DB instance if these sessions are in a stopped state. You can also add a schedule with a convenient interval to this query.

Querying extended event files

You can either use SQL Server Management Studio or the `sys.fn_xe_file_target_read_file` function to view data from extended events that use file targets. For more information on this function, see [sys.fn_xe_file_target_read_file \(Transact-SQL\)](#) in the Microsoft documentation.

Extended event file targets can only write files to the `D:\rdsdbdata\log` directory on RDS for SQL Server.

As an example, use the following SQL query to list the contents of all files of extended event sessions whose names start with `xe`.

```
SELECT * FROM sys.fn_xe_file_target_read_file('d:\rdsdbdata\log\xe*', null,null,null);
```

Access to transaction log backups with RDS for SQL Server

With access to transaction log backups for RDS for SQL Server, you can list the transaction log backup files for a database and copy them to a target Amazon S3 bucket. By copying transaction log backups in an Amazon S3 bucket, you can use them in combination with full and differential database backups to perform point in time database restores. You use RDS stored procedures to set up access to transaction log backups, list available transaction log backups, and copy them to your Amazon S3 bucket.

Access to transaction log backups provides the following capabilities and benefits:

- List and view the metadata of available transaction log backups for a database on an RDS for SQL Server DB instance.
- Copy available transaction log backups from RDS for SQL Server to a target Amazon S3 bucket.
- Perform point-in-time restores of databases without the need to restore an entire DB instance. For more information on restoring a DB instance to a point in time, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Availability and support

Access to transaction log backups is supported in all AWS Regions. Access to transaction log backups is available for all editions and versions of Microsoft SQL Server supported on Amazon RDS.

Requirements

The following requirements must be met before enabling access to transaction log backups:

- Automated backups must be enabled on the DB instance and the backup retention must be set to a value of one or more days. For more information on enabling automated backups and configuring a retention policy, see [Enabling automated backups \(p. 429\)](#).
- An Amazon S3 bucket must exist in the same account and Region as the source DB instance. Before enabling access to transaction log backups, choose an existing Amazon S3 bucket or [create a new bucket](#) to use for your transaction log backup files.
- An Amazon S3 bucket permissions policy must be configured as follows to allow Amazon RDS to copy transaction log files into it:
 1. Set the object account ownership property on the bucket to **Bucket Owner Preferred**.
 2. Add the following policy. There will be no policy by default, so use the bucket Access Control Lists (ACL) to edit the bucket policy and add it.

The following example uses an ARN to specify a resource. We recommend using the `SourceArn` and `SourceAccount` global condition context keys in resource-based trust relationships to limit the service's permissions to a specific resource. For more information on working with ARNs, see [Amazon resource names \(ARNs\)](#) and [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

Example of an Amazon S3 permissions policy for access to transaction log backups

```
{  
  {  
    "Version": "2012-10-17",  
    "Statement": [  
      {  
        "Sid": "Only allow writes to my bucket with bucket owner full control",  
        "Effect": "Allow",  
        "Principal": "arn:aws:s3:::mybucket",  
        "Action": "s3:PutObject",  
        "Resource": "arn:aws:s3:::mybucket/*"  
      }  
    ]  
  }  
}
```

```
"Effect": "Allow",
"Principal": {
    "Service": "backups.rds.amazonaws.com"
},
>Action": "s3:PutObject",
"Resource": "arn:aws:s3:::{customer_bucket}/{customer_path}/*",
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:sourceAccount": "{customer_account}",
        "aws:sourceArn": "{db_instance_arn}"
    }
}
]
}
```

- An AWS Identity and Access Management (IAM) role to access the Amazon S3 bucket. If you already have an IAM role, you can use that. You can choose to have a new IAM role created for you when you add the SQLSERVER_BACKUP_RESTORE option by using the AWS Management Console. Alternatively, you can create a new one manually. For more information on creating and configuring an IAM role with SQLSERVER_BACKUP_RESTORE, see [Manually creating an IAM role for native backup and restore \(p. 1102\)](#).
- The SQLSERVER_BACKUP_RESTORE option must be added to an option group on your DB instance. For more information on adding the SQLSERVER_BACKUP_RESTORE option, see [Support for native backup and restore in SQL Server \(p. 1214\)](#).

Note

If your DB instance has storage encryption enabled , the AWS KMS (KMS) actions and key must be provided in the IAM role provided in the native backup and restore option group.

Optionally, if you intend to use the `rds_restore_log` stored procedure to perform point in time database restores, we recommend using the same Amazon S3 path for the native backup and restore option group and access to transaction log backups. This method ensures that when Amazon RDS assumes the role from the option group to perform the restore log functions, it has access to retrieve transaction log backups from the same Amazon S3 path.

Limitations and recommendations

Access to transaction log backups has the following limitations and recommendations:

- You can list and copy up to the last seven days of transaction log backups for any DB instance that has backup retention configured between one to 35 days.
- The Amazon S3 bucket used for access to transaction log backups must exist in the same account and Region as the source DB instance. Cross-account and cross-region copy is not supported.
- Only one Amazon S3 bucket can be configured as a target to copy transaction log backups into. You can choose a new target Amazon S3 bucket with the `rds_tlog_copy_setup` stored procedure. For more information on choosing a new target Amazon S3 bucket, see [Setting up access to transaction log backups \(p. 1185\)](#).
- You cannot specify the KMS key when using the `rds_tlog_backup_copy_to_S3` stored procedure if your RDS instance is not enabled for storage encryption.
- Multi-account copying is not supported. The IAM role used for copying will only permit write access to Amazon S3 buckets within the owner account of the DB instance.
- Only two concurrent tasks of any type may be run on an RDS for SQL Server DB instance.
- Only one copy task can run for a single database at a given time. If you want to copy transaction log backups for multiple databases on the DB instance, use a separate copy task for each database.

- If you copy a transaction log backup that already exists with the same name in the Amazon S3 bucket, the existing transaction log backup will be overwritten.
- You can only run the stored procedures that are provided with access to transaction log backups on the primary DB instance. You can't run these stored procedures on an RDS for SQL Server read replica or on a secondary instance of a Multi-AZ DB cluster.
- If the RDS for SQL Server DB instance is rebooted while the `rds_tlog_backup_copy_to_S3` stored procedure is running, the task will automatically restart from the beginning when the DB instance is back online. Any transaction log backups that had been copied to the Amazon S3 bucket while the task was running before the reboot will be overwritten.
- The Microsoft SQL Server system databases and the RDSAdmin database cannot be configured for access to transaction log backups.

Setting up access to transaction log backups

To set up access to transaction log backups, complete the list of requirements in the [Requirements \(p. 1183\)](#) section, and then run the `rds_tlog_copy_setup` stored procedure. The procedure will enable the access to transaction log backups feature at the DB instance level. You don't need to run it for each individual database on the DB instance.

Important

The database user must be granted the `db_owner` role within SQL Server on each database to configure and use the access to transaction log backups feature.

Example usage:

```
exec msdb.dbo.rds_tlog_copy_setup  
@target_s3_arn='arn:aws:s3:::mybucket/myfolder';
```

The following parameter is required:

- `@target_s3_arn` – The ARN of the target Amazon S3 bucket to copy transaction log backups files to.

Example of setting an Amazon S3 target bucket:

```
exec msdb.dbo.rds_tlog_copy_setup @target_s3_arn='arn:aws:s3:::accesstlogs-testbucket/mytestdb1';
```

To validate the configuration, call the `rds_show_configuration` stored procedure.

Example of validating the configuration:

```
exec rdsadmin.dbo.rds_show_configuration @name='target_s3_arn_for_tlog_copy';
```

To modify access to transaction log backups to point to a different Amazon S3 bucket, you can view the current Amazon S3 bucket value and re-run the `rds_tlog_copy_setup` stored procedure using a new value for the `@target_s3_arn`.

Example of viewing the existing Amazon S3 bucket configured for access to transaction log backups

```
exec rdsadmin.dbo.rds_show_configuration @name='target_s3_arn_for_tlog_copy';
```

Example of updating to a new target Amazon S3 bucket

```
exec msdb.dbo.rds_tlog_copy_setup @target_s3_arn='arn:aws:s3:::mynewbucket/mynewfolder';
```

Listing available transaction log backups

With RDS for SQL Server, databases configured to use the full recovery model and a DB instance backup retention set to one or more days have transaction log backups automatically enabled. By enabling access to transaction log backups, up to seven days of those transaction log backups are made available for you to copy into your Amazon S3 bucket.

After you have enabled access to transaction log backups, you can start using it to list and copy available transaction log backup files.

Listing transaction log backups

To list all transaction log backups available for an individual database, call the `rds_fn_list_tlog_backup_metadata` function. You can use an `ORDER BY` or a `WHERE` clause when calling the function.

Example of listing and filtering available transaction log backup files

```
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename');
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename') WHERE
    rds_backup_seq_id = 3507;
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename') WHERE
    backup_file_time_utc > '2022-09-15 20:44:01' ORDER BY backup_file_time_utc DESC;
```

	db_name	db_id	family_guid	rds_backup_seq_id	backup_file_epoch	backup_file_name
1	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	43	1661846641	2022-09-15 20:44:01
2	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	44	1661846941	2022-09-15 20:44:01
3	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	45	1661847241	2022-09-15 20:44:01
4	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	46	1661847541	2022-09-15 20:44:01
5	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	47	1661847841	2022-09-15 20:44:01
6	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	48	1661848142	2022-09-15 20:44:01
7	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	49	1661848441	2022-09-15 20:44:01
8	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	50	1661848741	2022-09-15 20:44:01
9	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	51	1661849041	2022-09-15 20:44:01
10	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	52	1661849341	2022-09-15 20:44:01
11	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	53	1661849641	2022-09-15 20:44:01
12	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	54	1661849941	2022-09-15 20:44:01
13	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	55	1661850241	2022-09-15 20:44:01
14	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	56	1661850541	2022-09-15 20:44:01
15	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	57	1661850841	2022-09-15 20:44:01

The `rds_fn_list_tlog_backup_metadata` function returns the following output:

Column name	Data type	Description
<code>db_name</code>	<code>sysname</code>	The database name provided to list the transaction log backups for.
<code>db_id</code>	<code>int</code>	The internal database identifier for the input parameter <code>db_name</code> .
<code>family_guid</code>	<code>uniqueidentifier</code>	The unique ID of the original database at creation. This value remains the same when the database is restored, even to a different database name.
<code>rds_backup_seq_id</code>	<code>int</code>	The ID that RDS uses internally to maintain a sequence number for each transaction log backup file.
<code>backup_file_epoch</code>	<code>bigint</code>	The epoch time that a transaction backup file was generated.
<code>backup_file_time_utc</code>	<code>datetime</code>	The UTC time-converted value for the <code>backup_file_epoch</code> value.
<code>starting_lsn</code>	<code>numeric(25,0)</code>	The log sequence number of the first or oldest log record of a transaction log backup file.
<code>ending_lsn</code>	<code>numeric(25,0)</code>	The log sequence number of the last or next log record of a transaction log backup file.
<code>is_log_chain_broken</code>	<code>bit</code>	A boolean value indicating if the log chain is broken between the current transaction log backup file and the previous transaction log backup file.
<code>file_size_bytes</code>	<code>bigint</code>	The size of the transactional backup set in bytes.
<code>Error</code>	<code>varchar(4000)</code>	Error message if the <code>rds_fn_list_tlog_backup_metadata</code> function throws an exception. <code>NULL</code> if no exceptions.

Copying transaction log backups

To copy a set of available transaction log backups for an individual database to your Amazon S3 bucket, call the `rds_tlog_backup_copy_to_S3` stored procedure. The `rds_tlog_backup_copy_to_S3` stored procedure will initiate a new task to copy transaction log backups.

Note

The `rds_tlog_backup_copy_to_S3` stored procedure will copy the transaction log backups without validating against `is_log_chain_broken` attribute. For this reason, you should manually confirm an unbroken log chain before running the `rds_tlog_backup_copy_to_S3` stored procedure. For further explanation, see [Validating the transaction log backup log chain \(p. 1191\)](#).

Example usage of the `rds_tlog_backup_copy_to_S3` stored procedure

```
exec msdb.dbo.rds_tlog_backup_copy_to_S3
@db_name='mydbname',
[@kms_key_arn='arn:aws:kms:region:account-id:key/key-id'],
[@backup_file_start_time='2022-09-01 01:00:15'],
[@backup_file_end_time='2022-09-01 21:30:45'],
```

```
[@starting_lsn=149000000112100001],  
[@ending_lsn=149000000120400001],  
[@rds_backup_starting_seq_id=5],  
[@rds_backup_ending_seq_id=10];
```

The following input parameters are available:

Parameter	Description
@db_name	The name of the database to copy transaction log backups for
@kms_key_arn	The ARN of the KMS key used to encrypt a storage-encrypted DB instance.
@backup_file_start_time	The UTC timestamp as provided from the [backup_file_time_utc] column of the rds_fn_list_tlog_backup_metadata function.
@backup_file_end_time	The UTC timestamp as provided from the [backup_file_time_utc] column of the rds_fn_list_tlog_backup_metadata function.
@starting_lsn	The log sequence number (LSN) as provided from the [starting_lsn] column of the rds_fn_list_tlog_backup_metadata function
@ending_lsn	The log sequence number (LSN) as provided from the [ending_lsn] column of the rds_fn_list_tlog_backup_metadata function.
@rds_backup_starting_seq_id	The sequence ID as provided from the [rds_backup_seq_id] column of the rds_fn_list_tlog_backup_metadata function.
@rds_backup_ending_seq_id	The sequence ID as provided from the [rds_backup_seq_id] column of the rds_fn_list_tlog_backup_metadata function.

You can specify a set of either the time, LSN, or sequence ID parameters. Only one set of parameters are required.

You can also specify just a single parameter in any of the sets. For example, by providing a value for only the backup_file_end_time parameter, all available transaction log backup files prior to that time within the seven-day limit will be copied to your Amazon S3 bucket.

Following are the valid input parameter combinations for the rds_tlog_backup_copy_to_S3 stored procedure.

Parameters provided	Expected result
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name = 'testdb1', @backup_file_start_time='2022-08-23 00:00:00', @backup_file_end_time='2022-08-30 00:00:00';</pre>	Copies transaction log backups from the last seven days and exist between the provided range of backup_file_start_time and backup_file_end_time. In this example, the stored procedure will copy transaction

Parameters provided	Expected result
	log backups that were generated between '2022-08-23 00:00:00' and '2022-08-30 00:00:00'.
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_s3 @db_name = 'testdb1', @backup_file_start_time='2022-08-23 00:00:00';</pre>	Copies transaction log backups from the last seven days and starting from the provided backup_file_start_time. In this example, the stored procedure will copy transaction log backups from '2022-08-23 00:00:00' up to the latest transaction log backup.
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_s3 @db_name = 'testdb1', @backup_end_time='2022-08-30 00:00:00';</pre>	Copies transaction log backups from the last seven days up to the provided backup_file_end_time. In this example, the stored procedure will copy transaction log backups from '2022-08-23 00:00:00' up to '2022-08-30 00:00:00'.
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_s3 @db_name='testdb1', @starting_lsn =1490000000040007, @end_lsn = 1490000000050009;</pre>	Copies transaction log backups that are available from the last seven days and are between the provided range of the starting_lsn and ending_lsn. In this example, the stored procedure will copy transaction log backups from the last seven days with an LSN range between 1490000000040007 and 1490000000050009.

Parameters provided	Expected result
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @starting_lsn =1490000000040007;</pre>	Copies transaction log backups that are available from the last seven days, beginning from the provided starting_lsn. In this example, the stored procedure will copy transaction log backups from LSN 1490000000040007 up to the latest transaction log backup.
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @ending_lsn = 1490000000050009;</pre>	Copies transaction log backups that are available from the last seven days, up to the provided ending_lsn. In this example, the stored procedure will copy transaction log backups beginning from the last seven days up to lsn 1490000000050009.
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id=2000, @rds_backup_ending_seq_id=5000;</pre>	Copies transaction log backups that are available from the last seven days, and exist between the provided range of rds_backup_starting_seq_id and rds_backup_ending_seq_id. In this example, the stored procedure will copy transaction log backups beginning from the last seven days and within the provided rds backup sequence id range, starting from seq_id 2000 up to seq_id 5000.

Parameters provided	Expected result
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id=2000;</pre>	<p>Copies transaction log backups that are available from the last seven days, beginning from the provided <code>rds_backup_starting_seq_id</code>. In this example, the stored procedure will copy transaction log backups beginning from seq_id 2000, up to the latest transaction log backup.</p>
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_ending_seq_id=5000;</pre>	<p>Copies transaction log backups that are available from the last seven days, up to the provided <code>rds_backup_ending_seq_id</code>. In this example, the stored procedure will copy transaction log backups beginning from the last seven days, up to seq_id 5000.</p>
<pre>exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id=2000; @rds_backup_ending_seq_id=2000;</pre>	<p>Copies a single transaction log backup with the provided <code>rds_backup_starting_seq_id</code>, if available within the last seven days. In this example, the stored procedure will copy a single transaction log backup that has a seq_id of 2000, if it exists within the last seven days.</p>

Validating the transaction log backup log chain

Databases configured for access to transaction log backups must have automated backup retention enabled. Automated backup retention sets the databases on the DB instance to the FULL recovery model. To support point in time restore for a database, avoid changing the database recovery model, which can result in a broken log chain. We recommend keeping the database set to the FULL recovery model.

To manually validate the log chain before copying transaction log backups, call the `rds_fn_list_tlog_backup_metadata` function and review the values in the `is_log_chain_broken` column. A value of "1" indicates the log chain was broken between the current log backup and the previous log backup.

The following example shows a broken log chain in the output from the `rds_fn_list_tlog_backup_metadata` stored procedure.

rds_sequence_id	first_lsn	last_lsn	is_log_chain_broken
43	90023	90457	0
44	90457	90985	0
45	90987	92034	1

In a normal log chain, the log sequence number (LSN) value for `first_lsn` for given `rds_sequence_id` should match the value of `last_lsn` in the preceding `rds_sequence_id`. In the image, the `rds_sequence_id` of 45 has a `first_lsn` value 90987, which does not match the `last_lsn` value of 90985 for preceding `rds_sequence_id` 44.

For more information about SQL Server transaction log architecture and log sequence numbers, see [Transaction Log Logical Architecture](#) in the Microsoft SQL Server documentation.

Amazon S3 bucket folder and file structure

Transaction log backups have the following standard structure and naming convention within an Amazon S3 bucket:

- A new folder is created under the `target_s3_arn` path for each database with the naming structure as `{db_id}.{family_guid}`.
- Within the folder, transaction log backups have a filename structure as `{db_id}.{family_guid}.{rds_backup_seq_id}.{backup_file_epoch}`.
- You can view the details of `family_guid`, `db_id`, `rds_backup_seq_id` and `backup_file_epoch` with the `rds_fn_list_tlog_backup_metadata` function.

The following example shows the folder and file structure of a set of transaction log backups within an Amazon S3 bucket.

Amazon S3 > Buckets > rds-sql-server-kms-bucket > 10.36a85812-2b1e-47c6-b956-a020776fff66/

10.36a85812-2b1e-47c6-b956-a020776fff66/

Objects **Properties**

Objects (87)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For more information, see [Amazon S3 Inventory](#).

C **Copy S3 URI** **Copy URL** **Download** **Open** **Delete** **Actions**

Find objects by prefix

<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.0.1664557862	1664557862
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.1.1664558161	1664558161
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.2.1664558461	1664558461
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.3.1664558761	1664558761
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.4.1664559061	1664559061
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.5.1664559361	1664559361
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.6.1664559661	1664559661
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.7.1664559961	1664559961
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.8.1664560261	1664560261
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.9.1664560561	1664560561
<input type="checkbox"/>	10.36a85812-2b1e-47c6-b956-a020776fff66.10.1664560862	1664560862

Tracking the status of tasks

To track the status of your copy tasks, call the `rds_task_status` stored procedure. If you don't provide any parameters, the stored procedure returns the status of all tasks.

Example usage:

```
exec msdb.dbo.rds_task_status
@db_name='database_name',
@task_id=ID_number;
```

The following parameters are optional:

- `@db_name` – The name of the database to show the task status for.
- `@task_id` – The ID of the task to show the task status for.

Example of listing the status for a specific task ID:

```
exec msdb.dbo.rds_task_status @task_id=5;
```

Example of listing the status for a specific database and task:

```
exec msdb.dbo.rds_task_status@db_name='my_database',@task_id=5;
```

Example of listing all tasks and their status for a specific database:

```
exec msdb.dbo.rds_task_status @db_name='my_database';
```

Example of listing all tasks and their status on the current DB instance:

```
exec msdb.dbo.rds_task_status;
```

Canceling a task

To cancel a running task, call the `rds_cancel_task` stored procedure.

Example usage:

```
exec msdb.dbo.rds_cancel_task @task_id=ID_number;
```

The following parameter is required:

- `@task_id` – The ID of the task to cancel. You can view the task ID by calling the `rds_task_status` stored procedure.

For more information on viewing and canceling running tasks, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Troubleshooting access to transaction log backups

The following are issues you might encounter when you use the stored procedures for access to transaction log backups.

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
<code>rds_tlog_copy_start</code>	Backups are disabled on this DB instance. Enable DB instance backups with a retention of at least	Automated backups are not enabled for the DB instance.	DB instance backup retention must be enabled with a retention of at least one day. For more information on enabling automated backups and configuring backup retention, see Backup retention period (p. 429) .

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
	"1" and try again.		
rds_tlog_copy_setup	running the rds_tlog_copy_setup stored procedure. Reconnect to the RDS endpoint and try again.	An internal error occurred.	Reconnect to the RDS endpoint and run the rds_tlog_copy_setup stored procedure again.
rds_tlog_copy_setup	Attempting the rds_tlog_backup attempt setup stored procedure inside a transaction is not supported. Verify that the session has no open transactions and try again.	The stored procedure was attempted within a transaction using BEGIN and END.	Avoid using BEGIN and END when running the rds_tlog_copy_setup stored procedure.
rds_tlog_copy_setup	The S3 bucket name for the input parameter @target_s3_arn should contain at least one character other than a space.	An incorrect value was provided for the input parameter @target_s3_arn.	Ensure the input parameter @target_s3_arn specifies the complete Amazon S3 bucket ARN.
rds_tlog_copy_setup	The SQLSERVER_BACKUP_RESTORE option isn't enabled or is in the process of being enabled. Enable the option or try again later.	The SQLSERVER_BACKUP_RESTORE option is not enabled on the DB instance or was just enabled and pending internal activation.	Enable the SQLSERVER_BACKUP_RESTORE option as specified in the Requirements section. Wait a few minutes and run the rds_tlog_copy_setup stored procedure again.

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_copy_setup	The target S3 arn for the input parameter @target_s3_arn can't be empty or null.	An NULL value was provided for the input parameter @target_s3_arn, or the value wasn't provided.	Ensure the input parameter @target_s3_arn specifies the complete Amazon S3 bucket ARN.
rds_tlog_copy_setup	The target S3 arn for the input parameter @target_s3_arn must begin with arn:aws.	The input parameter @target_s3_arn was provide without arn:aws on the front.	Ensure the input parameter @target_s3_arn specifies the complete Amazon S3 bucket ARN.
rds_tlog_copy_setup	The target S3 ARN is already set to the provided value.	The rds_tlog_copy_setup stored procedure previously ran and was configured with an Amazon S3 bucket ARN.	To modify the Amazon S3 bucket value for access to transaction log backups, provide a different target S3 ARN.
rds_tlog_copy_setup	unable to generate credentials for enabling Access to Transaction Log Backups. Confirm the S3 path ARN provided with rds_tlog_copy_setup, and try again later.	There was an unspecified error while generating credentials to enable access to transaction log backups.	Review your setup configuration and try again.
rds_tlog_copy_setup	You cannot run the rds_tlog_copy stored procedure while there are pending tasks. Wait for the pending tasks to complete and try again.	Only two tasks may run at any time. There are pending tasks awaiting completion.	View pending tasks and wait for them to complete. For more information on monitoring task status, see Tracking the status of tasks (p. 1193) .

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup	A <code>_Copy_to_S3</code> backup file copy task has already been issued for database: %s with task Id: %d, please try again later.	Only one copy task may run at any time for a given database. There is a pending copy task awaiting completion.	View pending tasks and wait for them to complete. For more information on monitoring task status, see Tracking the status of tasks (p. 1193) .
rds_tlog_backup	At least one of these three parameter sets must be provided. SET-1: <code>(@backup_file_start_time,</code> <code>@backup_file_end_time)</code> SET-2: <code>(@starting_lsn,</code> <code>@ending_lsn)</code> SET-3: <code>(@rds_backup_starting_seq_id,</code> <code>@rds_backup_ending_seq_id)</code>	None of the three parameter sets were provided, or a provided parameter set is missing a required parameter.	You can specify either the time, lsn, or sequence ID parameters. One set from these three sets of parameters are required. For more information on required parameters, see Copying transaction log backups (p. 1187) .
rds_tlog_backup	Backup_start_lsn disabled on your instance. Please enable backups and try again in some time.	Automated backups are not enabled for the DB instance.	For more information on enabling automated backups and configuring backup retention, see Backup retention period (p. 429) .
rds_tlog_backup	<code>Copy_to_S3</code> the given database %s.	The value provided for input parameter @db_name does not match a database name on the DB instance.	Use the correct database name. To list all databases by name, run <code>SELECT * from sys.databases</code>
rds_tlog_backup	<code>Copy_to_S3</code> run the rds_tlog_backup stored procedure for SQL Server system databases or the rdsadmin database.	The value provided for input parameter @db_name matches a <code>SQLServerSystem</code> database name or the RDSAdmin database.	The following databases are not allowed to be used with access to transaction log backups: master, model, msdb, tempdb, RDSAdmin.

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup	<code>Database_S3</code> name for the input parameter @db_name can't be empty or null.	The value provided for input parameter @db_name was empty or NULL.	Use the correct database name. To list all databases by name, run <code>SELECT * from sys.databases</code>
rds_tlog_backup	<code>Drop_to_S3</code> backup retention period must be set to at least 1 to run the rds_tlog_backup_copy_setup stored procedure.	Automated backups are not enabled for the DB instance.	For more information on enabling automated backups and configuring backup retention, see Backup retention period (p. 429) .
rds_tlog_backup	<code>Copyutnig</code> the stored procedure rds_tlog_backup_copy_to_S3. Reconnect to the RDS endpoint and try again.	An internal error occurred.	Reconnect to the RDS endpoint and run the rds_tlog_backup_copy_to_S3 stored procedure again.
rds_tlog_backup	<code>Options_to_S3</code> these three parameter sets can be provided. SET-1: (@backup_file_start_time, @backup_file_end_time) SET-2: (@starting_lsn, @ending_lsn) SET-3: (@rds_backup_starting_seq_id, @rds_backup_ending_seq_id)	Multiple parameter sets were provided.	You can specify either the time, lsn, or sequence ID parameters. One set from these three sets of parameters are required. For more information on required parameters, see Copying transaction log backups (p. 1187) .

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup	Run point 163 rds_tlog_backup stored procedure inside a transaction is not supported. Verify that the session has no open transactions and try again.	The stored procedure was attempted within a transaction using BEGIN and END.	Avoid using BEGIN and END when running the rds_tlog_backup_copy_to_S3 stored procedure.
rds_tlog_backup	Run point 163 The provided parameters fall outside of the transaction backup log retention period. To list of available transaction log backup files, run the rds_fn_list_tlog_backup_metadata function.	There are no available transactional log backups for the provided input parameters that fit in the copy retention window.	Try again with a valid set of parameters. For more information on required parameters, see Copying transaction log backups (p. 1187) .
rds_tlog_backup	Run point 163 There was an S3 permissions error in processing the request. Ensure the bucket is in the same Account and Region as the DB Instance, and confirm the S3 bucket policy permissions against the template in the public documentation.	There was an issue detected with the provided S3 bucket or its policy permissions.	Confirm your setup for access to transaction log backups is correct. For more information on setup requirements for your S3 bucket, see Requirements (p. 1183) .

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup	<code>Procedure rds_tlog_backup cannot be run on a RDS read replica instance.</code>	The stored procedure was run on a RDS read replica instance.	Connect to the RDS primary DB instance to run the <code>rds_tlog_backup_copy_to_S3</code> stored procedure.
rds_tlog_backup	<code>The value provided for input parameter @starting_lsn must be less than @ending_lsn.</code>	The value provided for input parameter <code>@starting_lsn</code> was greater than the value provided for input parameter <code>@ending_lsn</code> .	Ensure the value provided for input parameter <code>@starting_lsn</code> is less than the value provided for input parameter <code>@ending_lsn</code> .
rds_tlog_backup	<code>The db_owner role has not been granted for the account attempting to run the rds_tlog_backup_copy_to_S3 stored procedure on the provided db_name.</code>	The <code>db_owner</code> role has not been granted for the account attempting to run the <code>rds_tlog_backup_copy_to_S3</code> stored procedure on the provided <code>db_name</code> .	Ensure the account running the stored procedure is permissioned with the <code>db_owner</code> role for the provided <code>db_name</code> .
rds_tlog_backup	<code>The provided ID for the input parameter @rds_backup_starting_seq_id must be less than or equal to @rds_backup_endng_seq_id.</code>	The value provided for input parameter <code>@rds_backup_starting_seq_id</code> was greater than the value provided for input parameter <code>@rds_backup_endng_seq_id</code> .	Ensure the value provided for input parameter <code>@rds_backup_starting_seq_id</code> is less than the value provided for input parameter <code>@rds_backup_endng_seq_id</code> .
rds_tlog_backup	<code>The SQLSERVER_BACKUP_RESTORE option isn't enabled or is in the process of being enabled. Enable the option or try again later.</code>	The <code>SQLSERVER_BACKUP_RESTORE</code> option is not enabled on the DB instance or was just enabled and pending internal activation.	Enable the <code>SQLSERVER_BACKUP_RESTORE</code> option as specified in the Requirements section. Wait a few minutes and run the <code>rds_tlog_backup_copy_to_S3</code> stored procedure again.

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup	The <code>@start_time</code> provided for input parameter <code>@backup_file_start_time</code> was greater than the value provided for input parameter <code>@backup_file_end_time</code> .	The value provided for input parameter <code>@backup_file_start_time</code> was greater than the value provided for input parameter <code>@backup_file_end_time</code> .	Ensure the value provided for input parameter <code>@backup_file_start_time</code> is less than the value provided for input parameter <code>@backup_file_end_time</code> .
rds_tlog_backup	We were unable to process the request due to a lack of access. Please check your setup and permissions for the feature.	There may be an issue with the Amazon S3 bucket permissions, or the Amazon S3 bucket provided is in another account or Region.	Ensure the Amazon S3 bucket policy permissions are permissioned to allow RDS access. Ensure the Amazon S3 bucket is in the same account and Region as the DB instance.
rds_tlog_backup	You must provide a KMS Key ARN as input parameter to the stored procedure for instances that are not storage-encrypted.	When storage encryption is not enabled on the DB instance, the input parameter <code>@kms_key_arn</code> should not be provided.	Do not provide an input parameter for <code>@kms_key_arn</code> .
rds_tlog_backup	You must provide a KMS Key ARN as input parameter to the stored procedure for storage encrypted instances.	When storage encryption is enabled on the DB instance, the input parameter <code>@kms_key_arn</code> must be provided.	Provide an input parameter for <code>@kms_key_arn</code> with a value that matches the ARN of the Amazon S3 bucket to use for transaction log backups.

Stored Procedure	Error Message	Issue	Troubleshooting suggestions
rds_tlog_backup_copy_to_S3	You must run the rds_tlog_copy_as_ebt procedure before attempting to run the rds_tlog_backup_copy_to_S3 stored procedure and set the @target_s3_arn, before running the rds_tlog_backup_copy_to_S3 stored procedure.	The access to transaction log backups setup procedure completed before attempting to run the rds_tlog_backup_copy_to_S3 stored procedure.	Run the rds_tlog_copy_setup stored procedure before running the rds_tlog_backup_copy_to_S3 stored procedure. For more information on running the setup procedure for access to transaction log backups, see Setting up access to transaction log backups (p. 1185) .

Options for the Microsoft SQL Server database engine

In this section, you can find descriptions for options that are available for Amazon RDS instances running the Microsoft SQL Server DB engine. To enable these options, you add them to an option group, and then associate the option group with your DB instance. For more information, see [Working with option groups \(p. 273\)](#).

If you're looking for optional features that aren't added through RDS option groups (such as SSL, Microsoft Windows Authentication, and Amazon S3 integration), see [Additional features for Microsoft SQL Server on Amazon RDS \(p. 1134\)](#).

Amazon RDS supports the following options for Microsoft SQL Server DB instances.

Option	Option ID	Engine editions
Linked Servers with Oracle OLEDB (p. 1206)	OLEDB_ORACLE	SQL Server Enterprise Edition SQL Server Standard Edition SQL Server Web Edition SQL Server Express Edition
Native backup and restore (p. 1214)	SQLSERVER_BACKUP_RESTORE	SQL Server Enterprise Edition SQL Server Standard Edition SQL Server Web Edition SQL Server Express Edition
Transparent Data Encryption (p. 1217)	TRANSPARENT_DATA_ENCRYPTION (RDS console) TDE (AWS CLI and RDS API)	SQL Server 2014–2019 Enterprise Edition SQL Server 2019 Standard Edition
SQL Server Audit (p. 1225)	SQLSERVER_AUDIT	In RDS, starting with SQL Server 2014, all editions of SQL Server support server-level audits, and Enterprise Edition also supports database-level audits. Starting with SQL Server SQL Server 2016 (13.x) SP1, all editions support both server-

Option	Option ID	Engine editions
		level and database-level audits. For more information, see SQL Server Audit (database engine) in the SQL Server documentation.
SQL Server Analysis Services (p. 1232)	SSAS	SQL Server Enterprise Edition SQL Server Standard Edition
SQL Server Integration Services (p. 1251)	SSIS	SQL Server Enterprise Edition SQL Server Standard Edition
SQL Server Reporting Services (p. 1266)	SSRS	SQL Server Enterprise Edition SQL Server Standard Edition
Microsoft Distributed Transaction Coordinator (p. 1279)	MSDTC	In RDS, starting with SQL Server 2014, all editions of SQL Server support distributed transactions.

Listing the available options for SQL Server versions and editions

You can use the `describe-option-group-options` AWS CLI command to list the available options for SQL Server versions and editions, and the settings for those options.

The following example shows the options and option settings for SQL Server 2019 Enterprise Edition. The `--engine-name` option is required.

```
aws rds describe-option-group-options --engine-name sqlserver-ee --major-engine-version 15.00
```

The output resembles the following:

```
{
    "OptionGroupOptions": [
        {
            "Name": "MSDTC",
            "Description": "Microsoft Distributed Transaction Coordinator",
            "EngineName": "sqlserver-ee",
            "MajorEngineVersion": "15.00",
            "MinimumRequiredMinorEngineVersion": "4043.16.v1",
            ...
        }
    ]
}
```

```
"PortRequired": true,
"DefaultPort": 5000,
"OptionsDependedOn": [],
"OptionsConflictsWith": [],
"Persistent": false,
"Permanent": false,
"RequiresAutoMinorEngineVersionUpgrade": false,
"VpcOnly": false,
"OptionGroupOptionSettings": [
    {
        "SettingName": "ENABLE_SNA_LU",
        "SettingDescription": "Enable support for SNA LU protocol",
        "DefaultValue": "true",
        "ApplyType": "DYNAMIC",
        "AllowedValues": "true,false",
        "IsModifiable": true,
        "IsRequired": false,
        "MinimumEngineVersionPerAllowedValue": []
    },
    ...
    {
        "Name": "TDE",
        "Description": "SQL Server - Transparent Data Encryption",
        "EngineName": "sqlserver-ee",
        "MajorEngineVersion": "15.00",
        "MinimumRequiredMinorEngineVersion": "4043.16.v1",
        "PortRequired": false,
        "OptionsDependedOn": [],
        "OptionsConflictsWith": [],
        "Persistent": true,
        "Permanent": false,
        "RequiresAutoMinorEngineVersionUpgrade": false,
        "VpcOnly": false,
        "OptionGroupOptionSettings": []
    }
]
```

Support for Linked Servers with Oracle OLEDB in Amazon RDS for SQL Server

Linked servers with the Oracle Provider for OLEDB on RDS for SQL Server lets you access external data sources on an Oracle database. You can read data from remote Oracle data sources and run commands against remote Oracle database servers outside of your RDS for SQL Server DB instance. Using linked servers with Oracle OLEDB, you can:

- Directly access data sources other than SQL Server
- Query against diverse Oracle data sources with the same query without moving the data
- Issue distributed queries, updates, commands, and transactions on data sources across an enterprise ecosystem
- Integrate connections to an Oracle database from within the Microsoft Business Intelligence suite (SSIS, SSRS, SSAS)
- Migrate from an Oracle database to RDS for SQL Server

You can activate one or more linked servers for Oracle on either an existing or new RDS for SQL Server DB instance. Then you can integrate external Oracle data sources with your DB instance.

Contents

- [Supported versions and Regions \(p. 1206\)](#)
- [Limitations and recommendations \(p. 1206\)](#)
- [Activating linked servers with Oracle \(p. 1207\)](#)
 - [Creating the option group for OLEDB_ORACLE \(p. 1207\)](#)
 - [Adding the OLEDB_ORACLE option to the option group \(p. 1208\)](#)
 - [Associating the option group with your DB instance \(p. 1209\)](#)
- [Modifying OLEDB provider properties \(p. 1210\)](#)
- [Modifying OLEDB driver properties \(p. 1211\)](#)
- [Deactivating linked servers with Oracle \(p. 1212\)](#)

Supported versions and Regions

RDS for SQL Server supports linked servers with Oracle OLEDB in all Regions for SQL Server Standard and Enterprise Editions on the following versions:

- SQL Server 2019, all versions
- SQL Server 2017, all versions

Linked servers with Oracle OLEDB is supported for the following Oracle Database versions:

- Oracle Database 21c, all versions
- Oracle Database 19c, all versions
- Oracle Database 18c, all versions

Limitations and recommendations

Keep in mind the following limitations and recommendations that apply to linked servers with Oracle OLEDB:

- Allow network traffic by adding the applicable TCP port in the security group for each RDS for SQL Server DB instance. For example, if you're configuring a linked server between an EC2 Oracle DB instance and an RDS for SQL Server DB instance, then you must allow traffic from the IP address of the EC2 Oracle DB instance. You also must allow traffic on the port that SQL Server is using to listen for database communication. For more information on security groups, see [Controlling access with security groups \(p. 2085\)](#).
- Perform a reboot of the RDS for SQL Server DB instance after turning on, turning off, or modifying the OLEDB_ORACLE option in your option group. The option group status displays pending_reboot for these events and is required.
- Only simple authentication is supported with a user name and password for the Oracle data source.
- Open Database Connectivity (ODBC) drivers are not supported. Only the latest version of the OLEDB driver is supported.
- Distributed transactions (XA) are supported. To activate distributed transactions, turn on the MSDTC option in the Option Group for your DB instance and make sure XA transactions are turned on. For more information, see [Support for Microsoft Distributed Transaction Coordinator in RDS for SQL Server \(p. 1279\)](#).
- Creating data source names (DSNs) to use as a shortcut for a connection string is not supported.
- OLEDB driver tracing is not supported. You can use SQL Server Extended Events to trace OLEDB events. For more information, see [Set up Extended Events in RDS for SQL Server](#).
- Access to the catalogs folder for an Oracle linked server is not supported using SQL Server Management Studio (SSMS).

Activating linked servers with Oracle

Activate linked servers with Oracle by adding the OLEDB_ORACLE option to your RDS for SQL Server DB instance. Use the following process:

1. Create a new option group, or choose an existing option group.
2. Add the OLEDB_ORACLE option to the option group.
3. Choose a version of the OLEDB driver to use.
4. Associate the option group with the DB instance.
5. Reboot the DB instance.

Creating the option group for OLEDB_ORACLE

To work with linked servers with Oracle, create an option group or modify an option group that corresponds to the SQL Server edition and version of the DB instance that you plan to use. To complete this procedure, use the AWS Management Console or the AWS CLI.

Console

The following procedure creates an option group for SQL Server Standard Edition 2019.

To create the option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** window, do the following:

- a. For **Name**, enter a name for the option group that is unique within your AWS account, such as **oracle-oledb-se-2019**. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, enter a brief description of the option group, such as **OLEDB_ORACLE option group for SQL Server SE 2019**. The description is used for display purposes.
 - c. For **Engine**, choose **sqlserver-se**.
 - d. For **Major engine version**, choose **15.00**.
5. Choose **Create**.

CLI

The following procedure creates an option group for SQL Server Standard Edition 2019.

To create the option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-option-group \
--option-group-name oracle-oledb-se-2019 \
--engine-name sqlserver-se \
--major-engine-version 15.00 \
--option-group-description "OLEDB_ORACLE option group for SQL Server SE 2019"
```

For Windows:

```
aws rds create-option-group ^
--option-group-name oracle-oledb-se-2019 ^
--engine-name sqlserver-se ^
--major-engine-version 15.00 ^
--option-group-description "OLEDB_ORACLE option group for SQL Server SE 2019"
```

Adding the OLEDB_ORACLE option to the option group

Next, use the AWS Management Console or the AWS CLI to add the OLEDB_ORACLE option to your option group.

Console

To add the OLEDB_ORACLE option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group that you just created, which is **oracle-oledb-se-2019** in this example.
4. Choose **Add option**.
5. Under **Option details**, choose **OLEDB_ORACLE** for **Option name**.
6. Under **Scheduling**, choose whether to add the option immediately or at the next maintenance window.
7. Choose **Add option**.

CLI

To add the OLEDB_ORACLE option

- Add the OLEDB_ORACLE option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name oracle-oledb-se-2019 \
--options OptionName=OLEDB_ORACLE \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name oracle-oledb-se-2019 ^
--options OptionName=OLEDB_ORACLE ^
--apply-immediately
```

Associating the option group with your DB instance

To associate the OLEDB_ORACLE option group and parameter group with your DB instance, use the AWS Management Console or the AWS CLI

Console

To finish activating linked servers for Oracle, associate your OLEDB_ORACLE option group with a new or existing DB instance:

- For a new DB instance, associate them when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, associate them by modifying the instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

You can associate the OLEDB_ORACLE option group and parameter group with a new or existing DB instance.

To create an instance with the OLEDB_ORACLE option group and parameter group

- Specify the same DB engine type and major version that you used when creating the option group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier mytestsqldatabaseoracleoledbinstance \
--db-instance-class db.m5.2xlarge \
--engine sqlserver-se \
--engine-version 15.0.4236.7.v1 \
--allocated-storage 100 \
--master-user-password secret123 \
```

```
--master-username admin \
--storage-type gp2 \
--license-model li \
--domain-iam-role-name my-directory-iam-role \
--domain my-domain-id \
--option-group-name oracleoledb-se-2019 \
--db-parameter-group-name my-parameter-group-name
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mytestsqserveroracleoledbinstance ^
--db-instance-class db.m5.2xlarge ^
--engine sqlserver-se ^
--engine-version 15.0.4236.7.v1 ^
--allocated-storage 100 ^
--master-user-password secret123 ^
--master-username admin ^
--storage-type gp2 ^
--license-model li ^
--domain-iam-role-name my-directory-iam-role ^
--domain my-domain-id ^
--option-group-name oracleoledb-se-2019 ^
--db-parameter-group-name my-parameter-group-name
```

To modify an instance and associate the OLEDB_ORACLE option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mytestsqserveroracleoledbinstance \
--option-group-name oracleoledb-se-2019 \
--db-parameter-group-name my-parameter-group-name \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mytestsqserveroracleoledbinstance ^
--option-group-name oracleoledb-se-2019 ^
--db-parameter-group-name my-parameter-group-name ^
--apply-immediately
```

Modifying OLEDB provider properties

You can view and change the properties of the OLEDB provider. Only the master user can perform this task. All linked servers for Oracle that are created on the DB instance use the same properties of that OLEDB provider. Call the sp_MSset_oleadb_prop stored procedure to change the properties of the OLEDB provider.

To change the OLEDB provider properties

```
USE [master]
GO
EXEC sp_MSset_oledb_prop N'OraOLEDB.Oracle', N'AllowInProcess', 1
EXEC sp_MSset_oledb_prop N'OraOLEDB.Oracle', N'DynamicParameters', 0
GO
```

The following properties can be modified:

Property name	Recommended Value (1 = On, 0 = Off)	Description
Dynamic parameter	1	Allows SQL placeholders (represented by "?") in parameterized queries.
Nested queries	1	Allows nested SELECT statements in the FROM clause, such as sub-queries.
Level zero only	0	Only base-level OLEDB interfaces are called against the provider.
Allow inprocess	1	If turned on, Microsoft SQL Server allows the provider to be instantiated as an in-process server. Set this property to 1 to use Oracle linked servers.
Non transacted updates	0	If non-zero, SQL Server allows updates.
Index as access path	False	If non-zero, SQL Server attempts to use indexes of the provider to fetch data.
Disallow adhoc access	False	If set, SQL Server does not allow running pass-through queries against the OLEDB provider. While this option can be checked, it is sometimes appropriate to run pass-through queries.
Supports LIKE operator	1	Indicates that the provider supports queries using the LIKE keyword.

Modifying OLEDB driver properties

You can view and change the properties of the OLEDB driver when creating a linked server for Oracle. Only the master user can perform this task. Driver properties define how the OLEDB driver handles data when working with a remote Oracle data source. Driver properties are specific to each Oracle linked server created on the DB instance. Call the master.dbo.sp_addlinkedserver stored procedure to change the properties of the OLEDB driver.

Example: To create a linked server and change the OLEDB driver FetchSize property

```
EXEC master.dbo.sp_addlinkedserver
@server = N'Oracle_link2',
@srvproduct=N'Oracle',
@provider=N'OraOLEDB.Oracle',
@datasrc=N'my-oracle-test.cnetsipka.us-west-2.rds.amazonaws.com:1521/ORCL',
@provstr='FetchSize=200'
GO
```

```
EXEC master.dbo.sp_addlinkedsvrlogin
@rmtsrvname=N'Oracle_link2',
@useself=N'False',
@locallogin=NULL,
@rmtnuser=N'master',
@rmtpassword='Test#1234'
GO
```

Deactivating linked servers with Oracle

To deactivate linked servers with Oracle, remove the OLEDB_ORACLE option from its option group.

Important

Removing the option doesn't delete the existing linked server configurations on the DB instance.

You must manually drop them to remove them from the DB instance.

You can reactivate the OLEDB_ORACLE option after removal to reuse the linked server configurations that were previously configured on the DB instance.

Console

The following procedure removes the OLEDB_ORACLE option.

To remove the OLEDB_ORACLE option from its option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the OLEDB_ORACLE option (oracle-oledb-se-2019 in the previous examples).
4. Choose **Delete option**.
5. Under **Deletion options**, choose **OLEDB_ORACLE** for **Options to delete**.
6. Under **Apply immediately**, choose **Yes** to delete the option immediately, or **No** to delete it during the next maintenance window.
7. Choose **Delete**.

CLI

The following procedure removes the OLEDB_ORACLE option.

To remove the OLEDB_ORACLE option from its option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
--option-group-name oracle-oledb-se-2019 \
--options OLEDB_ORACLE \
--apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
--option-group-name oracle-oledb-se-2019 ^
```

```
--options OLEDB_ORACLE ^
--apply-immediately
```

Support for native backup and restore in SQL Server

By using native backup and restore for SQL Server databases, you can create a differential or full backup of your on-premises database and store the backup files on Amazon S3. You can then restore to an existing Amazon RDS DB instance running SQL Server. You can also back up an RDS for SQL Server database, store it on Amazon S3, and restore it in other locations. In addition, you can restore the backup to an on-premises server, or a different Amazon RDS DB instance running SQL Server. For more information, see [Importing and exporting SQL Server databases using native backup and restore \(p. 1099\)](#).

Amazon RDS supports native backup and restore for Microsoft SQL Server databases by using differential and full backup files (.bak files).

Adding the native backup and restore option

The general process for adding the native backup and restore option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the SQLSERVER_BACKUP_RESTORE option to the option group.
3. Associate an AWS Identity and Access Management (IAM) role with the option. The IAM role must have access to an S3 bucket to store the database backups.

That is, the option must have as its option setting a valid Amazon Resource Name (ARN) in the format `arn:aws:iam::account-id:role/role-name`. For more information, see [Amazon Resource Names \(ARNs\)](#) in the *AWS General Reference*.

The IAM role must also have a trust relationship and a permissions policy attached. The trust relationship allows RDS to assume the role, and the permissions policy defines the actions that the role can perform. For more information, see [Manually creating an IAM role for native backup and restore \(p. 1102\)](#).

4. Associate the option group with the DB instance.

After you add the native backup and restore option, you don't need to restart your DB instance. As soon as the option group is active, you can begin backing up and restoring immediately.

Console

To add the native backup and restore option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Create a new option group or use an existing option group. For information on how to create a custom DB option group, see [Creating an option group \(p. 274\)](#).

To use an existing option group, skip to the next step.

4. Add the **SQLSERVER_BACKUP_RESTORE** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
5. Do one of the following:
 - To use an existing IAM role and Amazon S3 settings, choose an existing IAM role for **IAM Role**. If you use an existing IAM role, RDS uses the Amazon S3 settings configured for this role.
 - To create a new role and configure Amazon S3 settings, do the following:
 1. For **IAM role**, choose **Create a new role**.

2. For **S3 bucket**, choose an S3 bucket from the list.
3. For **S3 prefix (optional)**, specify a prefix to use for the files stored in your Amazon S3 bucket.

This prefix can include a file path but doesn't have to. If you provide a prefix, RDS attaches that prefix to all backup files. RDS then uses the prefix during a restore to identify related files and ignore irrelevant files. For example, you might use the S3 bucket for purposes besides holding backup files. In this case, you can use the prefix to have RDS perform native backup and restore only on a particular folder and its subfolders.

If you leave the prefix blank, then RDS doesn't use a prefix to identify backup files or files to restore. As a result, during a multiple-file restore, RDS attempts to restore every file in every folder of the S3 bucket.

4. Choose the **Enable encryption** check box to encrypt the backup file. Leave the check box cleared (the default) to have the backup file unencrypted.

If you chose **Enable encryption**, choose an encryption key for **AWS KMS key**. For more information about encryption keys, see [Getting started in the AWS Key Management Service Developer Guide](#).

6. Choose **Add option**.

7. Apply the option group to a new or existing DB instance:

- For a new DB instance, apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

This procedure makes the following assumptions:

- You're adding the SQLSERVER_BACKUP_RESTORE option to an option group that already exists. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
- You're associating the option with an IAM role that already exists and has access to an S3 bucket to store the backups.
- You're applying the option group to a DB instance that already exists. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

To add the native backup and restore option

1. Add the SQLSERVER_BACKUP_RESTORE option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--apply-immediately \
--option-group-name mybackupgroup \
--options "OptionName=SQLSERVER_BACKUP_RESTORE, \
OptionSettings=[{Name=IAM_ROLE_ARN,Value=arn:aws:iam::account-id:role/role-name}]"
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name mybackupgroup ^
```

```
--options "[{\\"OptionName\\": \\"SQLSERVER_BACKUP_RESTORE\\", ^  
\\\"OptionSettings\\": [{\\\"Name\\": \\"IAM_ROLE_ARN\\", ^  
\\\"Value\\": \"arn:aws:iam::account-id:role/role-name\"}]}]" ^  
--apply-immediately
```

Note

When using the Windows command prompt, you must escape double quotes ("") in JSON code by prefixing them with a backslash (\).

2. Apply the option group to the DB instance.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
  --db-instance-identifier mydbinstance \  
  --option-group-name mybackupgroup \  
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^  
  --db-instance-identifier mydbinstance ^  
  --option-group-name mybackupgroup ^  
  --apply-immediately
```

Modifying native backup and restore option settings

After you enable the native backup and restore option, you can modify the settings for the option. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#).

Removing the native backup and restore option

You can turn off native backup and restore by removing the option from your DB instance. After you remove the native backup and restore option, you don't need to restart your DB instance.

To remove the native backup and restore option from a DB instance, do one of the following:

- Remove the option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- Modify the DB instance and specify a different option group that doesn't include the native backup and restore option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Support for Transparent Data Encryption in SQL Server

Amazon RDS supports using Transparent Data Encryption (TDE) to encrypt stored data on your DB instances running Microsoft SQL Server. TDE automatically encrypts data before it is written to storage, and automatically decrypts data when the data is read from storage.

Amazon RDS supports TDE for the following SQL Server versions and editions:

- SQL Server 2019 Standard and Enterprise Editions
- SQL Server 2017 Enterprise Edition
- SQL Server 2016 Enterprise Edition
- SQL Server 2014 Enterprise Edition

Transparent Data Encryption for SQL Server provides encryption key management by using a two-tier key architecture. A certificate, which is generated from the database master key, is used to protect the data encryption keys. The database encryption key performs the actual encryption and decryption of data on the user database. Amazon RDS backs up and manages the database master key and the TDE certificate.

Transparent Data Encryption is used in scenarios where you need to encrypt sensitive data. For example, you might want to provide data files and backups to a third party, or address security-related regulatory compliance issues. You can't encrypt the system databases for SQL Server, such as the model or master databases.

A detailed discussion of Transparent Data Encryption is beyond the scope of this guide, but make sure that you understand the security strengths and weaknesses of each encryption algorithm and key. For information about Transparent Data Encryption for SQL Server, see [Transparent Data Encryption \(TDE\)](#) in the Microsoft documentation.

Topics

- [Turning on TDE for RDS for SQL Server \(p. 1217\)](#)
- [Encrypting data on RDS for SQL Server \(p. 1218\)](#)
- [Backing up and restoring TDE certificates on RDS for SQL Server \(p. 1219\)](#)
- [Backing up and restoring TDE certificates for on-premises databases \(p. 1222\)](#)
- [Turning off TDE for RDS for SQL Server \(p. 1224\)](#)

Turning on TDE for RDS for SQL Server

To turn on Transparent Data Encryption for an RDS for SQL Server DB instance, specify the TDE option in an RDS option group that's associated with that DB instance:

1. Determine whether your DB instance is already associated with an option group that has the TDE option. To view the option group that a DB instance is associated with, use the RDS console, the `describe-db-instance` AWS CLI command, or the API operation `DescribeDBInstances`.
2. If the DB instance isn't associated with an option group that has TDE turned on, you have two choices. You can create an option group and add the TDE option, or you can modify the associated option group to add it.

Note

In the RDS console, the option is named TRANSPARENT_DATA_ENCRYPTION. In the AWS CLI and RDS API, it's named TDE.

For information about creating or modifying an option group, see [Working with option groups \(p. 273\)](#). For information about adding an option to an option group, see [Adding an option to an option group \(p. 277\)](#).

3. Associate the DB instance with the option group that has the TDE option. For information about associating a DB instance with an option group, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Option group considerations

The TDE option is a persistent option. You can't remove it from an option group unless all DB instances and backups are no longer associated with the option group. After you add the TDE option to an option group, the option group can be associated only with DB instances that use TDE. For more information about persistent options in an option group, see [Option groups overview \(p. 273\)](#).

Because the TDE option is a persistent option, you can have a conflict between the option group and an associated DB instance. You can have a conflict in the following situations:

- The current option group has the TDE option, and you replace it with an option group that doesn't have the TDE option.
- You restore from a DB snapshot to a new DB instance that doesn't have an option group that contains the TDE option. For more information about this scenario, see [Option group considerations \(p. 463\)](#).

SQL Server performance considerations

Using Transparent Data Encryption can affect the performance of a SQL Server DB instance.

Performance for unencrypted databases can also be degraded if the databases are on a DB instance that has at least one encrypted database. As a result, we recommend that you keep encrypted and unencrypted databases on separate DB instances.

Encrypting data on RDS for SQL Server

When the TDE option is added to an option group, Amazon RDS generates a certificate that's used in the encryption process. You can then use the certificate to run SQL statements that encrypt data in a database on the DB instance.

The following example uses the RDS-created certificate called RDSTDECertificateName to encrypt a database called myDatabase.

```
----- Turning on TDE -----  
  
-- Find an RDS TDE certificate to use  
USE [master]  
GO  
SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'  
GO  
  
USE [myDatabase]  
GO  
-- Create a database encryption key (DEK) using one of the certificates from the previous  
step  
CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256  
ENCRYPTION BY SERVER CERTIFICATE [RDSTDECertificateName]  
GO  
  
-- Turn on encryption for the database  
ALTER DATABASE [myDatabase] SET ENCRYPTION ON  
GO
```

```
-- Verify that the database is encrypted
USE [master]
GO
SELECT name FROM sys.databases WHERE is_encrypted = 1
GO
SELECT db_name(database_id) as DatabaseName, * FROM sys.dm_database_encryption_keys
GO
```

The time that it takes to encrypt a SQL Server database using TDE depends on several factors. These include the size of the DB instance, whether the instance uses Provisioned IOPS storage, the amount of data, and other factors.

Backing up and restoring TDE certificates on RDS for SQL Server

RDS for SQL Server provides stored procedures for backing up, restoring, and dropping TDE certificates. RDS for SQL Server also provides a function for viewing restored user TDE certificates.

User TDE certificates are used to restore databases to RDS for SQL Server that are on-premises and have TDE turned on. These certificates have the prefix `UserTDECertificate_`. After restoring databases, and before making them available to use, RDS modifies the databases that have TDE turned on to use RDS-generated TDE certificates. These certificates have the prefix `RDSTDECertificate`.

User TDE certificates remain on the RDS for SQL Server DB instance, unless you drop them using the `rds_drop_tde_certificate` stored procedure. For more information, see [Dropping restored TDE certificates \(p. 1222\)](#).

You can use a user TDE certificate to restore other databases from the source DB instance. The databases to restore must use the same TDE certificate and have TDE turned on. You don't have to import (restore) the same certificate again.

Topics

- [Prerequisites \(p. 1219\)](#)
- [Limitations \(p. 1220\)](#)
- [Backing up a TDE certificate \(p. 1220\)](#)
- [Restoring a TDE certificate \(p. 1221\)](#)
- [Viewing restored TDE certificates \(p. 1221\)](#)
- [Dropping restored TDE certificates \(p. 1222\)](#)

Prerequisites

Before you can back up or restore TDE certificates on RDS for SQL Server, make sure to perform the following tasks. The first three are described in [Setting up for native backup and restore \(p. 1101\)](#).

1. Create Amazon S3 buckets for storing files to back up and restore.

We recommend that you use separate buckets for database backups and for TDE certificate backups.

2. Create an IAM role for backing up and restoring files.

The IAM role must be both a user and an administrator for the AWS KMS key.

In addition to the permissions required for SQL Server native backup and restore, the IAM role also requires the following permissions:

- `s3:GetBucketACL`, `s3:GetBucketLocation`, and `s3>ListBucket` on the S3 bucket resource
- `s3>ListAllMyBuckets` on the * resource

3. Add the `SQLSERVER_BACKUP_RESTORE` option to an option group on your DB instance.

This is in addition to the TRANSPARENT_DATA_ENCRYPTION (TDE) option.

4. Make sure that you have a symmetric encryption KMS key. You have the following options:
 - If you have an existing KMS key in your account, you can use it. No further action is necessary.
 - If you don't have an existing symmetric encryption KMS key in your account, create a KMS key by following the instructions in [Creating keys](#) in the *AWS Key Management Service Developer Guide*.

Limitations

Using stored procedures to back up and restore TDE certificates has the following limitations:

- Both the SQLSERVER_BACKUP_RESTORE and TRANSPARENT_DATA_ENCRYPTION (TDE) options must be added to the option group that you associated with your DB instance.
- TDE certificate backup and restore aren't supported on Multi-AZ DB instances.
- Canceling TDE certificate backup and restore tasks isn't supported.
- You can't use a user TDE certificate for TDE encryption of any other database on your RDS for SQL Server DB instance. You can use it to restore only other databases from the source DB instance that have TDE turned on and that use the same TDE certificate.
- You can drop only user TDE certificates.
- The maximum number of user TDE certificates supported on RDS is 10. If the number exceeds 10, drop unused TDE certificates and try again.
- The certificate name can't be empty or null.
- When restoring a certificate, the certificate name can't include the keyword RDSTDECERTIFICATE, and must start with the UserTDECertificate_ prefix.
- The @certificate_name parameter can include only the following characters: a-z, 0-9, @, \$, #, and underscore (_).
- The file extension for @certificate_file_s3_arn must be .cer (case-insensitive).
- The file extension for @private_key_file_s3_arn must be .pvk (case-insensitive).
- The S3 metadata for the private key file must include the x-amz-meta-rds-tde-pwd tag. For more information, see [Backing up and restoring TDE certificates for on-premises databases \(p. 1222\)](#).

Backing up a TDE certificate

To back up TDE certificates, use the rds_backup_tde_certificate stored procedure. It has the following syntax.

```
EXECUTE msdb.dbo.rds_backup_tde_certificate
    @certificate_name='UserTDECertificate_certificate_name | RDSTDECertificatetimestamp',
    @certificate_file_s3_arn='arn:aws:s3:::bucket_name/certificate_file_name.cer',
    @private_key_file_s3_arn='arn:aws:s3:::bucket_name/key_file_name.pvk',
    @kms_password_key_arn='arn:aws:kms:region:account-id:key/key-id',
    [@overwrite_s3_files=0/1];
```

The following parameters are required:

- @certificate_name – The name of the TDE certificate to back up.
- @certificate_file_s3_arn – The destination Amazon Resource Name (ARN) for the certificate backup file in Amazon S3.
- @private_key_file_s3_arn – The destination S3 ARN of the private key file that secures the TDE certificate.
- @kms_password_key_arn – The ARN of the symmetric KMS key used to encrypt the private key password.

The following parameter is optional:

- `@overwrite_s3_files` – Indicates whether to overwrite the existing certificate and private key files in S3:
 - 0 – Doesn't overwrite the existing files. This value is the default.
- Setting `@overwrite_s3_files` to 0 returns an error if a file already exists.
- 1 – Overwrites an existing file that has the specified name, even if it isn't a backup file.

Example of backing up a TDE certificate

```
EXECUTE msdb.dbo.rds_backup_tde_certificate
    @certificate_name='RDSTDECertificate20211115T185333',
    @certificate_file_s3_arn='arn:aws:s3:::TDE_certs/mycertfile.cer',
    @private_key_file_s3_arn='arn:aws:s3:::TDE_certs/mykeyfile.pvk',
    @kms_password_key_arn='arn:aws:kms:us-west-2:123456789012:key/AKIAIOSFODNN7EXAMPLE',
    @overwrite_s3_files=1;
```

Restoring a TDE certificate

You use the `rds_restore_tde_certificate` stored procedure to restore (import) user TDE certificates. It has the following syntax.

```
EXECUTE msdb.dbo.rds_restore_tde_certificate
    @certificate_name='UserTDECertificate_certificate_name',
    @certificate_file_s3_arn='arn:aws:s3:::bucket_name/certificate_file_name.cer',
    @private_key_file_s3_arn='arn:aws:s3:::bucket_name/key_file_name.pvk',
    @kms_password_key_arn='arn:aws:kms:region:account-id:key/key-id';
```

The following parameters are required:

- `@certificate_name` – The name of the TDE certificate to restore. The name must start with the `UserTDECertificate_` prefix.
- `@certificate_file_s3_arn` – The S3 ARN of the backup file used to restore the TDE certificate.
- `@private_key_file_s3_arn` – The S3 ARN of the private key backup file of the TDE certificate to be restored.
- `@kms_password_key_arn` – The ARN of the symmetric KMS key used to encrypt the private key password.

Example of restoring a TDE certificate

```
EXECUTE msdb.dbo.rds_restore_tde_certificate
    @certificate_name='UserTDECertificate_myTDECertificate',
    @certificate_file_s3_arn='arn:aws:s3:::TDE_certs/mycertfile.cer',
    @private_key_file_s3_arn='arn:aws:s3:::TDE_certs/mykeyfile.pvk',
    @kms_password_key_arn='arn:aws:kms:us-west-2:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Viewing restored TDE certificates

You use the `rds_fn_list_user_tde_certificates` function to view restored (imported) user TDE certificates. It has the following syntax.

```
SELECT * FROM msdb.dbo.rds_fn_list_user_tde_certificates();
```

The output resembles the following. Not all columns are shown here.

name	certificate_id	private_key_id	key_type	key_hex	object	start_date	expiry_date	private_key_last_backup
UserTDECertificate_tde_certificate	CERTIFICATE	ENCRYPTED	AnyCompliantR3KEY	Shipping57 a3 69 fd 1d 9e 47 2c 32 67 1d 9c ca af	0x6BB218B94C00B00080B04-0023-04-0BLL FE1BA2D866605006485B9:4510000000.0000000			

Dropping restored TDE certificates

To drop restored (imported) user TDE certificates that you aren't using, use the `rds_drop_tde_certificate` stored procedure. It has the following syntax.

```
EXECUTE msdb.dbo.rds_drop_tde_certificate
@certificate_name='UserTDECertificate_certificate_name';
```

The following parameter is required:

- `@certificate_name` – The name of the TDE certificate to drop.

You can drop only restored (imported) TDE certificates. You can't drop RDS-created certificates.

Example of dropping a TDE certificate

```
EXECUTE msdb.dbo.rds_drop_tde_certificate
@certificate_name='UserTDECertificate_myTDECertificate';
```

Backing up and restoring TDE certificates for on-premises databases

You can back up TDE certificates for on-premises databases, then later restore them to RDS for SQL Server. You can also restore an RDS for SQL Server TDE certificate to an on-premises DB instance.

The following procedure backs up a TDE certificate and private key. The private key is encrypted using a data key generated from your symmetric encryption KMS key.

To back up an on-premises TDE certificate

1. Generate the data key using the AWS CLI [generate-data-key](#) command.

```
aws kms generate-data-key \
--key-id my_KMS_key_ID \
--key-spec AES_256
```

The output resembles the following.

```
{
```

```
"CiphertextBlob": "AQIDAHiL2NEoA10Y6Bn7LJfnxi/OZe9kTQo/  
XQXduug1rmerwGiL7g5ux4av9GfZLxYTADATAAAAFjB8BgkqhkiG9w0B  
BwagbzBtAgEAMGgGCSqGSIB3DQEHAeBglghkgBZQMEAS4wEQQMyCxLMi7GRZgKqD65AgEQgDtjvZLJo2cQ31Vetngzm2ybHD  
2RezQy3sAS6ZHrCjfnnf0c65bFdhsXxjSMnudIY7AKw==",  
"Plaintext": "U/fpGtmzGCYBi8A2+0/9qcRQRK2zmG/aOn939ZnKi/0=",  
"KeyId": "arn:aws:kms:us-west-2:123456789012:key/1234abcd-00ee-99ff-88dd-aa11bb22cc33"  
}
```

You use the plain text output in the next step as the private key password.

2. Back up your TDE certificate as shown in the following example.

```
BACKUP CERTIFICATE myOnPremTDEcertificate TO FILE = 'D:\tde-cert-backup.cer'  
WITH PRIVATE KEY (  
FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\cert-  
backup-key.pvk',  
ENCRYPTION BY PASSWORD = 'U/fpGtmzGCYBi8A2+0/9qcRQRK2zmG/aOn939ZnKi/0=');
```

3. Save the certificate backup file to your Amazon S3 certificate bucket.
4. Save the private key backup file to your S3 certificate bucket, with the following tag in the file's metadata:
 - Key – *x-amz-meta-rds-tde-pwd*
 - Value – The CiphertextBlob value from generating the data key, as in the following example.

```
AQIDAHiL2NEoA10Y6Bn7LJfnxi/OZe9kTQo/  
XQXduug1rmerwGiL7g5ux4av9GfZLxYTADATAAAAFjB8BgkqhkiG9w0B  
BwagbzBtAgEAMGgGCSqGSIB3DQEHAeBglghkgBZQMEAS4wEQQMyCxLMi7GRZgKqD65AgEQgDtjvZLJo2cQ31Vetngzm2ybH  
2RezQy3sAS6ZHrCjfnnf0c65bFdhsXxjSMnudIY7AKw==
```

The following procedure restores an RDS for SQL Server TDE certificate to an on-premises DB instance. You copy and restore the TDE certificate on your destination DB instance using the certificate backup, corresponding private key file, and data key. The restored certificate is encrypted by the database master key of the new server.

To restore a TDE certificate

1. Copy the TDE certificate backup file and private key file from Amazon S3 to the destination instance.
2. Use your KMS key to decrypt the output cipher text to retrieve the plain text of the data key. The cipher text is located in the S3 metadata of the private key backup file.

```
aws kms decrypt \  
--key-id my_KMS_key_ID \  
--ciphertext-blob fileb://exampleCiphertextFile | base64 -d \  
--output text \  
--query Plaintext
```

You use the plain text output in the next step as the private key password.

3. Use the following SQL command to restore your TDE certificate.

```
CREATE CERTIFICATE myOnPremTDEcertificate FROM FILE='D:\tde-cert-backup.cer'  
WITH PRIVATE KEY (FILE = N'D:\tde-cert-key.pvk',  
DECRYPTION BY PASSWORD = 'plain_text_output');
```

For more information on KMS decryption, see [decrypt](#) in the KMS section of the *AWS CLI Command Reference*.

After the TDE certificate is restored on the destination DB instance, you can restore encrypted databases with that certificate.

Note

You can use the same TDE certificate to encrypt multiple SQL Server databases on the source DB instance. To migrate multiple databases to a destination instance, copy the TDE certificate associated with them to the destination instance only once.

Turning off TDE for RDS for SQL Server

To turn off TDE for an RDS for SQL Server DB instance, first make sure that there are no encrypted objects left on the DB instance. To do so, either decrypt the objects or drop them. If any encrypted objects exist on the DB instance, you can't turn off TDE for the DB instance. When you use the console to remove the TDE option from an option group, the console indicates that it's processing. In addition, an error event is created if the option group is associated with an encrypted DB instance or DB snapshot.

The following example removes the TDE encryption from a database called `customerDatabase`.

```
----- Removing TDE -----  
  
USE [customerDatabase]  
GO  
  
-- Turn off encryption of the database  
ALTER DATABASE [customerDatabase]  
SET ENCRYPTION OFF  
GO  
  
-- Wait until the encryption state of the database becomes 1. The state is 5 (Decryption in progress) for a while  
SELECT db_name(database_id) as DatabaseName, * FROM sys.dm_database_encryption_keys  
GO  
  
-- Drop the DEK used for encryption  
DROP DATABASE ENCRYPTION KEY  
GO  
  
-- Alter to SIMPLE Recovery mode so that your encrypted log gets truncated  
USE [master]  
GO  
ALTER DATABASE [customerDatabase] SET RECOVERY SIMPLE
```

When all objects are decrypted, you have two options:

1. You can modify the DB instance to be associated with an option group without the TDE option.
2. You can remove the TDE option from the option group.

SQL Server Audit

In Amazon RDS, you can audit Microsoft SQL Server databases by using the built-in SQL Server auditing mechanism. You can create audits and audit specifications in the same way that you create them for on-premises database servers.

RDS uploads the completed audit logs to your S3 bucket, using the IAM role that you provide. If you enable retention, RDS keeps your audit logs on your DB instance for the configured period of time.

For more information, see [SQL Server Audit \(database engine\)](#) in the Microsoft SQL Server documentation.

Topics

- [Support for SQL Server Audit \(p. 1225\)](#)
- [Adding SQL Server Audit to the DB instance options \(p. 1226\)](#)
- [Using SQL Server Audit \(p. 1227\)](#)
- [Viewing audit logs \(p. 1227\)](#)
- [Using SQL Server Audit with Multi-AZ instances \(p. 1228\)](#)
- [Configuring an S3 bucket \(p. 1228\)](#)
- [Manually creating an IAM role for SQL Server Audit \(p. 1229\)](#)

Support for SQL Server Audit

In Amazon RDS, starting with SQL Server 2014, all editions of SQL Server support server-level audits, and the Enterprise edition also supports database-level audits. Starting with SQL Server 2016 (13.x) SP1, all editions support both server-level and database-level audits. For more information, see [SQL Server Audit \(database engine\)](#) in the SQL Server documentation.

RDS supports configuring the following option settings for SQL Server Audit.

Option setting	Valid values	Description
IAM_ROLE_ARN	A valid Amazon Resource Name (ARN) in the format <code>arn:aws:iam::account-id:role/role-name</code> .	The ARN of the IAM role that grants access to the S3 bucket where you want to store your audit logs. For more information, see Amazon Resource Names (ARNs) in the AWS General Reference .
S3_BUCKET_ARN	A valid ARN in the format <code>arn:aws:s3:::bucket-name</code> or <code>arn:aws:s3:::bucket-name/key-prefix</code>	The ARN for the S3 bucket where you want to store your audit logs.
ENABLE_COMPRESSION	true or false	Controls audit log compression. By default, compression is enabled (set to true).
RETENTION_TIME	0 to 840	The retention time (in hours) that SQL Server audit records are kept on your RDS instance. By default, retention is disabled.

RDS supports SQL Server Audit in all AWS Regions except Middle East (Bahrain).

Adding SQL Server Audit to the DB instance options

Enabling SQL Server Audit requires two steps: enabling the option on the DB instance, and enabling the feature inside SQL Server. The process for adding the SQL Server Audit option to a DB instance is as follows:

1. Create a new option group, or copy or modify an existing option group.
2. Add and configure all required options.
3. Associate the option group with the DB instance.

After you add the SQL Server Audit option, you don't need to restart your DB instance. As soon as the option group is active, you can create audits and store audit logs in your S3 bucket.

To add and configure SQL Server Audit on a DB instance's option group

1. Choose one of the following:
 - Use an existing option group.
 - Create a custom DB option group and use that option group. For more information, see [Creating an option group \(p. 274\)](#).
2. Add the **SQLSERVER_AUDIT** option to the option group, and configure the option settings. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
 - For **IAM role**, if you already have an IAM role with the required policies, you can choose that role. To create a new IAM role, choose [Create a New Role](#). For information about the required policies, see [Manually creating an IAM role for SQL Server Audit \(p. 1229\)](#).
 - For **Select S3 destination**, if you already have an S3 bucket that you want to use, choose it. To create an S3 bucket, choose [Create a New S3 Bucket](#).
 - For **Enable Compression**, leave this option chosen to compress audit files. Compression is enabled by default. To disable compression, clear **Enable Compression**.
 - For **Audit log retention**, to keep audit records on the DB instance, choose this option. Specify a retention time in hours. The maximum retention time is 35 days.
3. Apply the option group to a new or existing DB instance. Choose one of the following:
 - If you are creating a new DB instance, apply the option group when you launch the instance.
 - On an existing DB instance, apply the option group by modifying the instance and then attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Modifying the SQL Server Audit option

After you enable the SQL Server Audit option, you can modify the settings. For information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#).

Removing SQL Server Audit from the DB instance options

You can turn off the SQL Server Audit feature by disabling audits and then deleting the option.

To remove auditing

1. Disable all of the audit settings inside SQL Server. To learn where audits are running, query the SQL Server security catalog views. For more information, see [Security catalog views](#) in the Microsoft SQL Server documentation.

2. Delete the SQL Server Audit option from the DB instance. Choose one of the following:
 - Delete the SQL Server Audit option from the option group that the DB instance uses. This change affects all DB instances that use the same option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
 - Modify the DB instance, and then choose an option group without the SQL Server Audit option. This change affects only the DB instance that you modify. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
3. After you delete the SQL Server Audit option from the DB instance, you don't need to restart the instance. Remove unneeded audit files from your S3 bucket.

Using SQL Server Audit

You can control server audits, server audit specifications, and database audit specifications the same way that you control them for on-premises database servers.

Creating audits

You create server audits in the same way that you create them for on-premises database servers. For information about how to create server audits, see [CREATE SERVER AUDIT](#) in the Microsoft SQL Server documentation.

To avoid errors, adhere to the following limitations:

- Don't exceed the maximum number of supported server audits per instance of 50.
- Instruct SQL Server to write data to a binary file.
- Don't use RDS_ as a prefix in the server audit name.
- For FILEPATH, specify D:\rdsdbdata\SQLAudit.
- For MAXSIZE, specify a size between 2 MB and 50 MB.
- Don't configure MAX_ROLLOVER_FILES or MAX_FILES.
- Don't configure SQL Server to shut down the DB instance if it fails to write the audit record.

Creating audit specifications

You create server audit specifications and database audit specifications the same way that you create them for on-premises database servers. For information about creating audit specifications, see [CREATE SERVER AUDIT SPECIFICATION](#) and [CREATE DATABASE AUDIT SPECIFICATION](#) in the Microsoft SQL Server documentation.

To avoid errors, don't use RDS_ as a prefix in the name of the database audit specification or server audit specification.

Viewing audit logs

Your audit logs are stored in D:\rdsdbdata\SQLAudit.

After SQL Server finishes writing to an audit log file—when the file reaches its size limit—Amazon RDS uploads the file to your S3 bucket. If retention is enabled, Amazon RDS moves the file into the retention folder: D:\rdsdbdata\SQLAudit\transmitted.

For information about configuring retention, see [Adding SQL Server Audit to the DB instance options \(p. 1226\)](#).

Audit records are kept on the DB instance until the audit log file is uploaded. You can view the audit records by running the following command.

```
SELECT *
FROM msdb.dbo.rds_fn_get_audit_file
('D:\rdsdbdata\SQLAudit\*.sqlaudit'
, default
, default )
```

You can use the same command to view audit records in your retention folder by changing the filter to D:\rdsdbdata\SQLAudit\transmitted*.sqlaudit.

```
SELECT *
FROM msdb.dbo.rds_fn_get_audit_file
('D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit'
, default
, default )
```

Using SQL Server Audit with Multi-AZ instances

For Multi-AZ instances, the process for sending audit log files to Amazon S3 is similar to the process for Single-AZ instances. However, there are some important differences:

- Database audit specification objects are replicated to all nodes.
- Server audits and server audit specifications aren't replicated to secondary nodes. Instead, you have to create or modify them manually.

To capture server audits or a server audit specification from both nodes:

1. Create a server audit or a server audit specification on the primary node.
2. Fail over to the secondary node and create a server audit or a server audit specification with the same name and GUID on the secondary node. Use the AUDIT_GUID parameter to specify the GUID.

Configuring an S3 bucket

The audit log files are automatically uploaded from the DB instance to your S3 bucket. The following restrictions apply to the S3 bucket that you use as a target for audit files:

- It must be in the same AWS Region as the DB instance.
- It must not be open to the public.
- It can't use [S3 Object Lock](#).
- The bucket owner must also be the IAM role owner.

The target key that is used to store the data follows this naming schema: bucket-name/key-prefix/instance-name/audit-name/node_file-name.ext

Note

You set both the bucket name and the key prefix values with the (S3_BUCKET_ARN) option setting.

The schema is composed of the following elements:

- **bucket-name** – The name of your S3 bucket.
- **key-prefix** – The custom key prefix you want to use for audit logs.

- **instance-name** – The name of your Amazon RDS instance.
- **audit-name** – The name of the audit.
- **node** – The identifier of the node that is the source of the audit logs (node1 or node2). There is one node for a Single-AZ instance and two replication nodes for a Multi-AZ instance. These are not primary and secondary nodes, because the roles of primary and secondary change over time. Instead, the node identifier is a simple label.
 - **node1** – The first replication node (Single-AZ has one node only).
 - **node2** – The second replication node (Multi-AZ has two nodes).
- **file-name** – The target file name. The file name is taken as-is from SQL Server.
- **ext** – The extension of the file (zip or sqlaudit):
 - **zip** – If compression is enabled (default).
 - **sqlaudit** – If compression is disabled.

Manually creating an IAM role for SQL Server Audit

Typically, when you create a new option, the AWS Management Console creates the IAM role and the IAM trust policy for you. However, you can manually create a new IAM role to use with SQL Server Audits, so that you can customize it with any additional requirements you might have. To do this, you create an IAM role and delegate permissions so that the Amazon RDS service can use your Amazon S3 bucket. When you create this IAM role, you attach trust and permissions policies. The trust policy allows Amazon RDS to assume this role. The permission policy defines the actions that this role can do. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *AWS Identity and Access Management User Guide*.

You can use the examples in this section to create the trust relationships and permissions policies you need.

The following example shows a trust relationship for SQL Server Audit. It uses the *service principal* `rds.amazonaws.com` to allow RDS to write to the S3 bucket. A *service principal* is an identifier that is used to grant permissions to a service. Anytime you allow access to `rds.amazonaws.com` in this way, you are allowing RDS to perform an action on your behalf. For more information about service principals, see [AWS JSON policy elements: Principal](#).

Example trust relationship for SQL Server Audit

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "rds.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based trust relationships to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the trust relationship, make sure to use the `aws:SourceArn` global condition context key with the full Amazon Resource Name (ARN) of the resources accessing the role. For SQL Server Audit, make sure to include both the DB option group and the DB instances, as shown in the following example.

Example trust relationship with global condition context key for SQL Server Audit

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [
                        "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier",
                        "arn:aws:rds:Region:my_account_ID:og:option_group_name"
                    ]
                }
            }
        }
    ]
}
```

In the following example of a permissions policy for SQL Server Audit, we specify an ARN for the Amazon S3 bucket. You can use ARNs to identify a specific account, user, or role that you want grant access to. For more information about using ARNs, see [Amazon resource names \(ARNs\)](#).

Example permissions policy for SQL Server Audit

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3>ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3>ListBucket",
                "s3:GetBucketACL",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::<bucket_name>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3>PutObject",
                "s3>ListMultipartUploadParts",
                "s3>AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::<bucket_name>/*"
        }
    ]
}
```

```
        "Resource": "arn:aws:s3:::bucket_name/key_prefix/*"
    }
]
```

Note

The s3>ListAllMyBuckets action is required for verifying that the same AWS account owns both the S3 bucket and the SQL Server DB instance. The action lists the names of the buckets in the account.

S3 bucket namespaces are global. If you accidentally delete your bucket, another user can create a bucket with the same name in a different account. Then the SQL Server Audit data is written to the new bucket.

Support for SQL Server Analysis Services in Amazon RDS for SQL Server

Microsoft SQL Server Analysis Services (SSAS) is part of the Microsoft Business Intelligence (MSBI) suite. SSAS is an online analytical processing (OLAP) and data mining tool that is installed within SQL Server. You use SSAS to analyze data to help make business decisions. SSAS differs from the SQL Server relational database because SSAS is optimized for queries and calculations common in a business intelligence environment.

You can turn on SSAS for existing or new DB instances. It's installed on the same DB instance as your database engine. For more information on SSAS, see the Microsoft [Analysis services documentation](#).

Amazon RDS supports SSAS for SQL Server Standard and Enterprise Editions on the following versions:

- Tabular mode:
 - SQL Server 2019, version 15.00.4043.16.v1 and higher
 - SQL Server 2017, version 14.00.3223.3.v1 and higher
 - SQL Server 2016, version 13.00.5426.0.v1 and higher
- Multidimensional mode:
 - SQL Server 2017, version 14.00.3381.3.v1 and higher
 - SQL Server 2016, version 13.00.5882.1.v1 and higher

Contents

- [Limitations \(p. 1232\)](#)
- [Turning on SSAS \(p. 1233\)](#)
 - [Creating an option group for SSAS \(p. 1233\)](#)
 - [Adding the SSAS option to the option group \(p. 1234\)](#)
 - [Associating the option group with your DB instance \(p. 1236\)](#)
 - [Allowing inbound access to your VPC security group \(p. 1237\)](#)
 - [Enabling Amazon S3 integration \(p. 1237\)](#)
- [Deploying SSAS projects on Amazon RDS \(p. 1237\)](#)
- [Monitoring the status of a deployment task \(p. 1238\)](#)
- [Using SSAS on Amazon RDS \(p. 1240\)](#)
 - [Setting up a Windows-authenticated user for SSAS \(p. 1240\)](#)
 - [Adding a domain user as a database administrator \(p. 1241\)](#)
 - [Creating an SSAS proxy \(p. 1242\)](#)
 - [Scheduling SSAS database processing using SQL Server Agent \(p. 1243\)](#)
 - [Revoking SSAS access from the proxy \(p. 1244\)](#)
- [Backing up an SSAS database \(p. 1245\)](#)
- [Restoring an SSAS database \(p. 1245\)](#)
 - [Restoring a DB instance to a specified time \(p. 1245\)](#)
- [Changing the SSAS mode \(p. 1246\)](#)
- [Turning off SSAS \(p. 1247\)](#)
- [Troubleshooting SSAS issues \(p. 1248\)](#)

Limitations

The following limitations apply to using SSAS on RDS for SQL Server:

- RDS for SQL Server supports running SSAS in Tabular or Multidimensional mode. For more information, see [Comparing tabular and multidimensional solutions](#) in the Microsoft documentation.
- You can only use one SSAS mode at a time. Before changing modes, make sure to delete all of the SSAS databases.

For more information, see [Changing the SSAS mode \(p. 1246\)](#).

- Multidimensional mode isn't supported on SQL Server 2019.
- Multi-AZ instances aren't supported.
- Instances must use AWS Directory Service for Microsoft Active Directory for SSAS authentication.
- Users aren't given SSAS server administrator access, but they can be granted database-level administrator access.
- The only supported port for accessing SSAS is 2383.
- You can't deploy projects directly. We provide an RDS stored procedure to do this. For more information, see [Deploying SSAS projects on Amazon RDS \(p. 1237\)](#).
- Processing during deployment isn't supported.
- Using .xma files for deployment isn't supported.
- SSAS project input files and database backup output files can only be in the D:\S3 folder on the DB instance.

Turning on SSAS

Use the following process to turn on SSAS for your DB instance:

1. Create a new option group, or choose an existing option group.
2. Add the SSAS option to the option group.
3. Associate the option group with the DB instance.
4. Allow inbound access to the virtual private cloud (VPC) security group for the SSAS listener port.
5. Turn on Amazon S3 integration.

Creating an option group for SSAS

Use the AWS Management Console or the AWS CLI to create an option group that corresponds to the SQL Server engine and version of the DB instance that you plan to use.

Note

You can also use an existing option group if it's for the correct SQL Server engine and version.

Console

The following console procedure creates an option group for SQL Server Standard Edition 2017.

To create the option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** pane, do the following:
 - a. For **Name**, enter a name for the option group that is unique within your AWS account, such as **ssas-se-2017**. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, enter a brief description of the option group, such as **SSAS option group for SQL Server SE 2017**. The description is used for display purposes.

- c. For **Engine**, choose **sqlserver-se**.
- d. For **Major engine version**, choose **14.00**.
5. Choose **Create**.

CLI

The following CLI example creates an option group for SQL Server Standard Edition 2017.

To create the option group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-option-group \
--option-group-name ssas-se-2017 \
--engine-name sqlserver-se \
--major-engine-version 14.00 \
--option-group-description "SSAS option group for SQL Server SE 2017"
```

For Windows:

```
aws rds create-option-group ^
--option-group-name ssas-se-2017 ^
--engine-name sqlserver-se ^
--major-engine-version 14.00 ^
--option-group-description "SSAS option group for SQL Server SE 2017"
```

Adding the SSAS option to the option group

Next, use the AWS Management Console or the AWS CLI to add the SSAS option to the option group.

Console

To add the SSAS option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group that you just created.
4. Choose **Add option**.
5. Under **Option details**, choose **SSAS** for **Option name**.
6. Under **Option settings**, do the following:

- a. For **Max memory**, enter a value in the range 10–80.

Max memory specifies the upper threshold above which SSAS begins releasing memory more aggressively to make room for requests that are running, and also new high-priority requests. The number is a percentage of the total memory of the DB instance. The allowed values are 10–80, and the default is 45.

- b. For **Mode**, choose the SSAS server mode, **Tabular** or **Multidimensional**.

If you don't see the **Mode** option setting, it means that Multidimensional mode isn't supported in your AWS Region. For more information, see [Limitations \(p. 1232\)](#).

Tabular is the default.

- c. For **Security groups**, choose the VPC security group to associate with the option.

Note

The port for accessing SSAS, 2383, is prepopulated.

7. Under **Scheduling**, choose whether to add the option immediately or at the next maintenance window.
8. Choose **Add option**.

[CLI](#)

To add the SSAS option

1. Create a JSON file, for example `ssas-option.json`, with the following parameters:
 - OptionGroupName – The name of option group that you created or chose previously (`ssas-se-2017` in the following example).
 - Port – The port that you use to access SSAS. The only supported port is 2383.
 - VpcSecurityGroupMemberships – Memberships for VPC security groups for your RDS DB instance.
 - MAX_MEMORY – The upper threshold above which SSAS should begin releasing memory more aggressively to make room for requests that are running, and also new high-priority requests. The number is a percentage of the total memory of the DB instance. The allowed values are 10–80, and the default is 45.
 - MODE – The SSAS server mode, either Tabular or Multidimensional. Tabular is the default.

If you receive an error that the MODE option setting isn't valid, it means that Multidimensional mode isn't supported in your AWS Region. For more information, see [Limitations \(p. 1232\)](#).

The following is an example of a JSON file with SSAS option settings.

```
{  
  "OptionGroupName": "ssas-se-2017",  
  "OptionsToInclude": [  
    {  
      "OptionName": "SSAS",  
      "Port": 2383,  
      "VpcSecurityGroupMemberships": ["sg-0abcdef123"],  
      "OptionSettings": [{"Name": "MAX_MEMORY", "Value": "60"},  
        {"Name": "MODE", "Value": "Multidimensional"}]  
    },  
    "ApplyImmediately": true  
  ]}
```

2. Add the SSAS option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
```

```
--cli-input-json file://ssas-option.json \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--cli-input-json file://ssas-option.json ^
--apply-immediately
```

Associating the option group with your DB instance

You can use the console or the CLI to associate the option group with your DB instance.

Console

Associate your option group with a new or existing DB instance:

- For a new DB instance, associate the option group with the DB instance when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, modify the instance and associate the new option group with it. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

If you use an existing instance, it must already have an Active Directory domain and AWS Identity and Access Management (IAM) role associated with it. If you create a new instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

CLI

You can associate your option group with a new or existing DB instance.

Note

If you use an existing instance, it must already have an Active Directory domain and IAM role associated with it. If you create a new instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

To create a DB instance that uses the option group

- Specify the same DB engine type and major version that you used when creating the option group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier myssasinstance \
--db-instance-class db.m5.2xlarge \
--engine sqlserver-se \
--engine-version 14.00.3223.3.v1 \
--allocated-storage 100 \
--master-user-password secret123 \
--master-username admin \
--storage-type gp2 \
--license-model li \
--domain-iam-role-name my-directory-iam-role \
--domain my-domain-id \
```

```
--option-group-name ssas-se-2017
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier myssasinstance ^
--db-instance-class db.m5.2xlarge ^
--engine sqlserver-se ^
--engine-version 14.00.3223.3.v1 ^
--allocated-storage 100 ^
--master-user-password secret123 ^
--master-username admin ^
--storage-type gp2 ^
--license-model li ^
--domain-iam-role-name my-directory-iam-role ^
--domain my-domain-id ^
--option-group-name ssas-se-2017
```

To modify a DB instance to associate the option group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier myssasinstance \
--option-group-name ssas-se-2017 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier myssasinstance ^
--option-group-name ssas-se-2017 ^
--apply-immediately
```

Allowing inbound access to your VPC security group

Create an inbound rule for the specified SSAS listener port in the VPC security group associated with your DB instance. For more information about setting up security groups, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

Enabling Amazon S3 integration

To download model configuration files to your host for deployment, use Amazon S3 integration. For more information, see [Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 \(p. 1153\)](#).

Deploying SSAS projects on Amazon RDS

On RDS, you can't deploy SSAS projects directly by using SQL Server Management Studio (SSMS). To deploy projects, use an RDS stored procedure.

Note

Using .xmla files for deployment isn't supported.

Before you deploy projects, make sure of the following:

- Amazon S3 integration is turned on. For more information, see [Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 \(p. 1153\)](#).
- The Processing Option configuration setting is set to Do Not Process. This setting means that no processing happens after deployment.
- You have both the *myssasproject*.asdatabase and *myssasproject*.deploymentoptions files. They're automatically generated when you build the SSAS project.

To deploy an SSAS project on RDS

1. Download the .asdatabase (SSAS model) file from your S3 bucket to your DB instance, as shown in the following example. For more information on the download parameters, see [Downloading files from an Amazon S3 bucket to a SQL Server DB instance \(p. 1160\)](#).

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.asdatabase',
[@rds_file_path='D:\S3\imyssasproject.asdatabase'],
[@overwrite_file=1];
```

2. Download the .deploymentoptions file from your S3 bucket to your DB instance.

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.deploymentoptions',
[@rds_file_path='D:\S3\imyssasproject.deploymentoptions'],
[@overwrite_file=1];
```

3. Deploy the project.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_DEPLOY_PROJECT',
@file_path='D:\S3\imyssasproject.asdatabase';
```

Monitoring the status of a deployment task

To track the status of your deployment (or download) task, call the `rds_fn_task_status` function. It takes two parameters. The first parameter should always be NULL because it doesn't apply to SSAS. The second parameter accepts a task ID.

To see a list of all tasks, set the first parameter to NULL and the second parameter to 0, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

To get a specific task, set the first parameter to NULL and the second parameter to the task ID, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

The `rds_fn_task_status` function returns the following information.

Output parameter	Description
task_id	The ID of the task.

Output parameter	Description
task_type	<p>For SSAS, tasks can have the following task types:</p> <ul style="list-style-type: none"> • SSAS_DEPLOY_PROJECT • SSAS_ADD_DB_ADMIN_MEMBER • SSAS_BACKUP_DB • SSAS_RESTORE_DB
database_name	Not applicable to SSAS tasks.
% complete	The progress of the task as a percentage.
duration (mins)	The amount of time spent on the task, in minutes.
lifecycle	<p>The status of the task. Possible statuses are the following:</p> <ul style="list-style-type: none"> • CREATED – After you call one of the SSAS stored procedures, a task is created and the status is set to CREATED. • IN_PROGRESS – After a task starts, the status is set to IN_PROGRESS. It can take up to five minutes for the status to change from CREATED to IN_PROGRESS. • SUCCESS – After a task completes, the status is set to SUCCESS. • ERROR – If a task fails, the status is set to ERROR. For more information about the error, see the task_info column. • CANCEL_REQUESTED – After you call <code>rds_cancel_task</code>, the status of the task is set to CANCEL_REQUESTED. • CANCELLED – After a task is successfully canceled, the status of the task is set to CANCELLED.
task_info	<p>Additional information about the task. If an error occurs during processing, this column contains information about the error.</p> <p>For more information, see Troubleshooting SSAS issues (p. 1248).</p>
last_updated	The date and time that the task status was last updated.
created_at	The date and time that the task was created.
S3_object_arn	Not applicable to SSAS tasks.
overwrite_S3_backup_file	Not applicable to SSAS tasks.
KMS_master_key_arn	Not applicable to SSAS tasks.
filepath	Not applicable to SSAS tasks.

Output parameter	Description
overwrite_file	Not applicable to SSAS tasks.
task_metadata	Metadata associated with the SSAS task.

Using SSAS on Amazon RDS

After deploying the SSAS project, you can directly process the OLAP database on SSMS.

To use SSAS on RDS

1. In SSMS, connect to SSAS using the user name and password for the Active Directory domain.
2. Expand **Databases**. The newly deployed SSAS database appears.
3. Locate the connection string, and update the user name and password to give access to the source SQL database. Doing this is required for processing SSAS objects.
 - a. For Tabular mode, do the following:
 1. Expand the **Connections** tab.
 2. Open the context (right-click) menu for the connection object, and then choose **Properties**.
 3. Update the user name and password in the connection string.
 - b. For Multidimensional mode, do the following:
 1. Expand the **Data Sources** tab.
 2. Open the context (right-click) menu for the data source object, and then choose **Properties**.
 3. Update the user name and password in the connection string.
4. Open the context (right-click) menu for the SSAS database that you created and choose **Process Database**.

Depending on the size of the input data, the processing operation might take several minutes to complete.

Topics

- [Setting up a Windows-authenticated user for SSAS \(p. 1240\)](#)
- [Adding a domain user as a database administrator \(p. 1241\)](#)
- [Creating an SSAS proxy \(p. 1242\)](#)
- [Scheduling SSAS database processing using SQL Server Agent \(p. 1243\)](#)
- [Revoking SSAS access from the proxy \(p. 1244\)](#)

Setting up a Windows-authenticated user for SSAS

The main administrator user (sometimes called the master user) can use the following code example to set up a Windows-authenticated login and grant the required procedure permissions. Doing this grants permissions to the domain user to run SSAS customer tasks, use S3 file transfer procedures, create credentials, and work with the SQL Server Agent proxy. For more information, see [Credentials \(database engine\)](#) and [Create a SQL Server Agent proxy](#) in the Microsoft documentation.

You can grant some or all of the following permissions as needed to Windows-authenticated users.

Example

```
-- Create a server-level domain user login, if it doesn't already exist
```

```

USE [master]
GO
CREATE LOGIN [mydomain\user_name] FROM WINDOWS
GO

-- Create domain user, if it doesn't already exist
USE [msdb]
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]
GO

-- Grant necessary privileges to the domain user
USE [master]
GO
GRANT ALTER ANY CREDENTIAL TO [mydomain\user_name]
GO

USE [msdb]
GO
GRANT EXEC ON msdb.dbo.rds_msbi_task TO [mydomain\user_name] with grant option
GRANT SELECT ON msdb.dbo.rds_fn_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_cancel_task TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_download_from_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_upload_to_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_delete_from_filesystem TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_gather_file_details TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_add_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_update_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_grant_login_to_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_revoke_login_from_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_delete_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_login_for_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_proxy_for_subsystem TO [mydomain\user_name] with grant
option
GRANT EXEC ON msdb.dbo.rds_sqlagent_proxy TO [mydomain\user_name] with grant option
ALTER ROLE [SQLAgentUserRole] ADD MEMBER [mydomain\user_name]
GO

```

Adding a domain user as a database administrator

You can add a domain user as an SSAS database administrator in the following ways:

- A database administrator can use SSMS to create a role with admin privileges, then add users to that role.
- You can use the following stored procedure.

```

exec msdb.dbo.rds_msbi_task
@task_type='SSAS_ADD_DB_ADMIN_MEMBER',
@database_name='myssasdb',
@ssas_role_name='exampleRole',
@ssas_role_member='domain_name\domain_user_name';

```

The following parameters are required:

- **@task_type** – The type of the MSBI task, in this case SSAS_ADD_DB_ADMIN_MEMBER.
- **@database_name** – The name of the SSAS database to which you're granting administrator privileges.
- **@ssas_role_name** – The SSAS database administrator role name. If the role doesn't already exist, it's created.
- **@ssas_role_member** – The SSAS database user that you're adding to the administrator role.

Creating an SSAS proxy

To be able to schedule SSAS database processing using SQL Server Agent, create an SSAS credential and an SSAS proxy. Run these procedures as a Windows-authenticated user.

To create the SSAS credential

- Create the credential for the proxy. To do this, you can use SSMS or the following SQL statement.

```
USE [master]
GO
CREATE CREDENTIAL [SSAS_Credential] WITH IDENTITY = N'mydomain\user_name', SECRET =
N'mysecret'
GO
```

Note

IDENTITY must be a domain-authenticated login. Replace *mysecret* with the password for the domain-authenticated login.

To create the SSAS proxy

1. Use the following SQL statement to create the proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_add_proxy
    @proxy_name=N'SSAS_Proxy',@credential_name=N'SSAS_Credential',@description=N''
GO
```

2. Use the following SQL statement to grant access to the proxy to other users.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_grant_login_to_proxy
    @proxy_name=N'SSAS_Proxy',@login_name=N'mydomain\user_name'
GO
```

3. Use the following SQL statement to give the SSAS subsystem access to the proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
    @task_type='GRANT_SUBSYSTEM_ACCESS',@proxy_name='SSAS_Proxy',@proxy_subsystem='SSAS'
GO
```

To view the proxy and grants on the proxy

1. Use the following SQL statement to view the grantees of the proxy.

```
USE [msdb]
GO
EXEC sp_help_proxy
GO
```

2. Use the following SQL statement to view the subsystem grants.

```
USE [msdb]
```

```
GO
EXEC msdb.dbo.sp_enum_proxy_for_subsystem
GO
```

Scheduling SSAS database processing using SQL Server Agent

After you create the credential and proxy and grant SSAS access to the proxy, you can create a SQL Server Agent job to schedule SSAS database processing.

To schedule SSAS database processing

- Use SSMS or T-SQL for creating the SQL Server Agent job. The following example uses T-SQL. You can further configure its job schedule through SSMS or T-SQL.
 - The @command parameter outlines the XML for Analysis (XMLA) command to be run by the SQL Server Agent job. This example configures SSAS Multidimensional database processing.
 - The @server parameter outlines the target SSAS server name of the SQL Server Agent job.

To call the SSAS service within the same RDS DB instance where the SQL Server Agent job resides, use localhost:2383.

To call the SSAS service from outside the RDS DB instance, use the RDS endpoint. You can also use the Kerberos Active Directory (AD) endpoint (*your-DB-instance-name.your-AD-domain-name*) if the RDS DB instances are joined by the same domain. For external DB instances, make sure to properly configure the VPC security group associated with the RDS DB instance for a secure connection.

You can further edit the query to support various XMLA operations. Make edits either by directly modifying the T-SQL query or by using the SSMS UI following SQL Server Agent job creation.

```
USE [msdb]
GO
DECLARE @jobId BINARY(16)
EXEC msdb.dbo.sp_add_job @job_name=N'SSAS_Job',
    @enabled=1,
    @notify_level_eventlog=0,
    @notify_level_email=0,
    @notify_level_netsend=0,
    @notify_level_page=0,
    @delete_level=0,
    @category_name=N'[Uncategorized (Local)]',
    @job_id = @jobId OUTPUT
GO
EXEC msdb.dbo.sp_add_jobserver
    @job_name=N'SSAS_Job',
    @server_name = N'(local)'
GO
EXEC msdb.dbo.sp_add_jobstep @job_name=N'SSAS_Job', @step_name=N'Process_SSAS_Object',
    @step_id=1,
    @cmdexec_success_code=0,
    @on_success_action=1,
    @on_success_step_id=0,
    @on_fail_action=2,
    @on_fail_step_id=0,
    @retry_attempts=0,
    @retry_interval=0,
    @os_run_priority=0, @subsystem=N'ANALYSISCOMMAND',
    @command=N'<Batch xmlns="http://schemas.microsoft.com/analysisservices/2003/
engine">
    <Parallel>
```

```

<Process xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ddl2="http://schemas.microsoft.com/analysisservices/2003/engine/2"
    xmlns:ddl2_2="http://schemas.microsoft.com/analysisservices/2003/engine/2/2"
    xmlns:ddl100_100="http://schemas.microsoft.com/analysisservices/2008/engine/100/100"
    xmlns:ddl200="http://schemas.microsoft.com/analysisservices/2010/engine/200"
    xmlns:ddl200_200="http://schemas.microsoft.com/analysisservices/2010/engine/200/200"
    xmlns:ddl1300="http://schemas.microsoft.com/analysisservices/2011/engine/300"
    xmlns:ddl1300_300="http://schemas.microsoft.com/analysisservices/2011/engine/300/300"
    xmlns:ddl1400="http://schemas.microsoft.com/analysisservices/2012/engine/400"
    xmlns:ddl1400_400="http://schemas.microsoft.com/analysisservices/2012/engine/400/400"
    xmlns:ddl1500="http://schemas.microsoft.com/analysisservices/2013/engine/500"
    xmlns:ddl1500_500="http://schemas.microsoft.com/analysisservices/2013/engine/500/500">
    <Object>
        <DatabaseID>Your_SSAS_Database_ID</DatabaseID>
    </Object>
    <Type>ProcessFull</Type>
    <WriteBackTableCreation>UseExisting</WriteBackTableCreation>
    </Process>
</Parallel>
</Batch>',
@server=N'localhost:2383',
@database_name=N'master',
@flags=0,
@proxy_name=N'SSAS_Proxy'
GO

```

Revoking SSAS access from the proxy

You can revoke access to the SSAS subsystem and delete the SSAS proxy using the following stored procedures.

To revoke access and delete the proxy

1. Revoke subsystem access.

```

USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
    @task_type='REVOKE_SUBSYSTEM_ACCESS',@proxy_name='SSAS_Proxy',@proxy_subsystem='SSAS'
GO

```

2. Revoke the grants on the proxy.

```

USE [msdb]
GO
EXEC msdb.dbo.sp_revoke_login_from_proxy
    @proxy_name=N'SSAS_Proxy',@name=N'mydomain\user_name'
GO

```

3. Delete the proxy.

```

USE [msdb]
GO
EXEC dbo.sp_delete_proxy @proxy_name = N'SSAS_Proxy'
GO

```

Backing up an SSAS database

You can create SSAS database backup files only in the D:\S3 folder on the DB instance. To move the backup files to your S3 bucket, use Amazon S3.

You can back up an SSAS database as follows:

- A domain user with the admin role for a particular database can use SSMS to back up the database to the D:\S3 folder.

For more information, see [Adding a domain user as a database administrator \(p. 1241\)](#).

- You can use the following stored procedure. This stored procedure doesn't support encryption.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_BACKUP_DB',
@database_name='myssasdb',
@file_path='D:\S3\ssas_db_backup.abf',
[@ssas_apply_compression=1],
[@ssas_overwrite_file=1];
```

The following parameters are required:

- @task_type – The type of the MSBI task, in this case SSAS_BACKUP_DB.
- @database_name – The name of the SSAS database that you're backing up.
- @file_path – The path for the SSAS backup file. The .abf extension is required.

The following parameters are optional:

- @ssas_apply_compression – Whether to apply SSAS backup compression. Valid values are 1 (Yes) and 0 (No).
- @ssas_overwrite_file – Whether to overwrite the SSAS backup file. Valid values are 1 (Yes) and 0 (No).

Restoring an SSAS database

Use the following stored procedure to restore an SSAS database from a backup.

You can't restore a database if there is an existing SSAS database with the same name. The stored procedure for restoring doesn't support encrypted backup files.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_RESTORE_DB',
@database_name='mynewssasdb',
@file_path='D:\S3\ssas_db_backup.abf';
```

The following parameters are required:

- @task_type – The type of the MSBI task, in this case SSAS_RESTORE_DB.
- @database_name – The name of the new SSAS database that you're restoring to.
- @file_path – The path to the SSAS backup file.

Restoring a DB instance to a specified time

Point-in-time recovery (PITR) doesn't apply to SSAS databases. If you do PITR, only the SSAS data in the last snapshot before the requested time is available on the restored instance.

To have up-to-date SSAS databases on a restored DB instance

1. Back up your SSAS databases to the D:\S3 folder on the source instance.
2. Transfer the backup files to the S3 bucket.
3. Transfer the backup files from the S3 bucket to the D:\S3 folder on the restored instance.
4. Run the stored procedure to restore the SSAS databases onto the restored instance.

You can also reprocess the SSAS project to restore the databases.

Changing the SSAS mode

You can change the mode in which SSAS runs, either Tabular or Multidimensional. To change the mode, use the AWS Management Console or the AWS CLI to modify the options settings in the SSAS option.

Important

You can only use one SSAS mode at a time. Make sure to delete all of the SSAS databases before changing the mode, or you receive an error.

Console

The following Amazon RDS console procedure changes the SSAS mode to Tabular and sets the MAX_MEMORY parameter to 70 percent.

To modify the SSAS option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the SSAS option that you want to modify (ssas-se-2017 in the previous examples).
4. Choose **Modify option**.
5. Change the option settings:
 - a. For **Max memory**, enter **70**.
 - b. For **Mode**, choose **Tabular**.
6. Choose **Modify option**.

AWS CLI

The following AWS CLI example changes the SSAS mode to Tabular and sets the MAX_MEMORY parameter to 70 percent.

For the CLI command to work, make sure to include all of the required parameters, even if you're not modifying them.

To modify the SSAS option

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
```

```
--option-group-name ssas-se-2017 \
--options
"OptionName=SSAS,VpcSecurityGroupMemberships=sg-12345e67,OptionSettings=[{Name=MAX_MEMORY,Value=70}
{Name=MODE,Value=Tabular}]" \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name ssas-se-2017 ^
--options
OptionName=SSAS,VpcSecurityGroupMemberships=sg-12345e67,OptionSettings=[{Name=MAX_MEMORY,Value=70}
{Name=MODE,Value=Tabular}] ^
--apply-immediately
```

Turning off SSAS

To turn off SSAS, remove the SSAS option from its option group.

Important

Before you remove the SSAS option, delete your SSAS databases.

We highly recommend that you back up your SSAS databases before deleting them and removing the SSAS option.

Console

To remove the SSAS option from its option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the SSAS option that you want to remove (ssas-se-2017 in the previous examples).
4. Choose **Delete option**.
5. Under **Deletion options**, choose **SSAS** for **Options to delete**.
6. Under **Apply immediately**, choose **Yes** to delete the option immediately, or **No** to delete it at the next maintenance window.
7. Choose **Delete**.

AWS CLI

To remove the SSAS option from its option group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
--option-group-name ssas-se-2017 \
--options SSAS \
--apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
--option-group-name ssas-se-2017 ^
--options SSAS ^
--apply-immediately
```

Troubleshooting SSAS issues

You might encounter the following issues when using SSAS.

Issue	Type	Troubleshooting suggestions
Unable to configure the SSAS option. The requested SSAS mode is <i>new_mode</i> , but the current DB instance has <i>number current_mode</i> databases. Delete the existing databases before switching to <i>new_mode</i> mode. To regain access to <i>current_mode</i> mode for database deletion, either update the current DB option group, or attach a new option group with %s as the MODE option setting value for the SSAS option.	RDS event	You can't change the SSAS mode if you still have SSAS databases that use the current mode. Delete the SSAS databases, then try again.
Unable to remove the SSAS option because there are <i>number</i> existing <i>mode</i> databases. The SSAS option can't be removed until all SSAS databases are deleted. Add the SSAS option again, delete all SSAS databases, and try again.	RDS event	You can't turn off SSAS if you still have SSAS databases. Delete the SSAS databases, then try again.
The SSAS option isn't enabled or is in the process of being enabled. Try again later.	RDS stored procedure	You can't run SSAS stored procedures when the option is turned off, or when it's being turned on.
The SSAS option is configured incorrectly. Make sure that the option group membership status is "in-sync", and review the RDS event logs for relevant SSAS configuration error messages. Following these investigations, try again. If errors continue to occur, contact AWS Support.	RDS stored procedure	<p>You can't run SSAS stored procedures when your option group membership isn't in the <i>in-sync</i> status. This puts the SSAS option in an incorrect configuration state.</p> <p>If your option group membership status changes to <i>failed</i> due to SSAS option modification, there are two possible reasons:</p> <ol style="list-style-type: none"> 1. The SSAS option was removed without the SSAS databases being deleted. 2. The SSAS mode was updated from Tabular to Multidimensional, or from Multidimensional to Tabular, without the existing SSAS databases being deleted. <p>Reconfigure the SSAS option, because RDS allows only one SSAS mode at a time, and doesn't support SSAS option removal with SSAS databases present.</p>

Issue	Type	Troubleshooting suggestions
		Check the RDS event logs for configuration errors for your SSAS instance, and resolve the issues accordingly.
Deployment failed. The change can only be deployed on a server running in <i>deployment_file_mode</i> mode. The current server mode is <i>current_mode</i> .	RDS stored procedure	<p>You can't deploy a Tabular database to a Multidimensional server, or a Multidimensional database to a Tabular server.</p> <p>Make sure that you're using files with the correct mode, and verify that the MODE option setting is set to the appropriate value.</p>
The restore failed. The backup file can only be restored on a server running in <i>restore_file_mode</i> mode. The current server mode is <i>current_mode</i> .	RDS stored procedure	<p>You can't restore a Tabular database to a Multidimensional server, or a Multidimensional database to a Tabular server.</p> <p>Make sure that you're using files with the correct mode, and verify that the MODE option setting is set to the appropriate value.</p>
The restore failed. The backup file and the RDS DB instance versions are incompatible.	RDS stored procedure	<p>You can't restore an SSAS database with a version incompatible to the SQL Server instance version.</p> <p>For more information, see Compatibility levels for tabular models and Compatibility level of a multidimensional database in the Microsoft documentation.</p>
The restore failed. The backup file specified in the restore operation is damaged or is not an SSAS backup file. Make sure that @rds_file_path is correctly formatted.	RDS stored procedure	<p>You can't restore an SSAS database with a damaged file.</p> <p>Make sure that the file isn't damaged or corrupted.</p> <p>This error can also be raised when @rds_file_path isn't correctly formatted (for example, it has double backslashes as in D:\\S3\\\\incorrect_format.abf).</p>
The restore failed. The restored database name can't contain any reserved words or invalid characters: . , ; ' ` : / \\ * ? \ " & % \$! + = () [] { } < >, or be longer than 100 characters.	RDS stored procedure	<p>The restored database name can't contain any reserved words or characters that aren't valid, or be longer than 100 characters.</p> <p>For SSAS object naming conventions, see Object naming rules in the Microsoft documentation.</p>
An invalid role name was provided. The role name can't contain any reserved strings.	RDS stored procedure	<p>The role name can't contain any reserved strings.</p> <p>For SSAS object naming conventions, see Object naming rules in the Microsoft documentation.</p>

Issue	Type	Troubleshooting suggestions
An invalid role name was provided. The role name can't contain any of the following reserved characters: . , ; ' ` : / \\ * ? \^ & % \$! + = () [] { } < >	RDS stored procedure	The role name can't contain any reserved characters. For SSAS object naming conventions, see Object naming rules in the Microsoft documentation.

Support for SQL Server Integration Services in Amazon RDS for SQL Server

Microsoft SQL Server Integration Services (SSIS) is a component that you can use to perform a broad range of data migration tasks. SSIS is a platform for data integration and workflow applications. It features a data warehousing tool used for data extraction, transformation, and loading (ETL). You can also use this tool to automate maintenance of SQL Server databases and updates to multidimensional cube data.

SSIS projects are organized into packages saved as XML-based .dtsx files. Packages can contain control flows and data flows. You use data flows to represent ETL operations. After deployment, packages are stored in SQL Server in the SSISDB database. SSISDB is an online transaction processing (OLTP) database in the full recovery mode.

Amazon RDS for SQL Server supports running SSIS directly on an RDS DB instance. You can enable SSIS on an existing or new DB instance. SSIS is installed on the same DB instance as your database engine.

RDS supports SSIS for SQL Server Standard and Enterprise Editions on the following versions:

- SQL Server 2019, version 15.00.4043.16.v1 and higher
- SQL Server 2017, version 14.00.3223.3.v1 and higher
- SQL Server 2016, version 13.00.5426.0.v1 and higher

Contents

- [Limitations and recommendations \(p. 1251\)](#)
- [Enabling SSIS \(p. 1253\)](#)
 - [Creating the option group for SSIS \(p. 1253\)](#)
 - [Adding the SSIS option to the option group \(p. 1254\)](#)
 - [Creating the parameter group for SSIS \(p. 1255\)](#)
 - [Modifying the parameter for SSIS \(p. 1256\)](#)
 - [Associating the option group and parameter group with your DB instance \(p. 1256\)](#)
 - [Enabling S3 integration \(p. 1258\)](#)
- [Administrative permissions on SSISDB \(p. 1258\)](#)
 - [Setting up a Windows-authenticated user for SSIS \(p. 1258\)](#)
- [Deploying an SSIS project \(p. 1259\)](#)
- [Monitoring the status of a deployment task \(p. 1260\)](#)
- [Using SSIS \(p. 1261\)](#)
 - [Setting database connection managers for SSIS projects \(p. 1261\)](#)
 - [Creating an SSIS proxy \(p. 1262\)](#)
 - [Scheduling an SSIS package using SQL Server Agent \(p. 1263\)](#)
 - [Revoking SSIS access from the proxy \(p. 1263\)](#)
- [Disabling SSIS \(p. 1264\)](#)
- [Dropping the SSISDB database \(p. 1265\)](#)

Limitations and recommendations

The following limitations and recommendations apply to running SSIS on RDS for SQL Server:

- The DB instance must use AWS Managed Microsoft AD for SSIS authentication.

- The DB instance must have an associated parameter group with the `clr_enabled` parameter set to 1. For more information, see [Modifying the parameter for SSIS \(p. 1256\)](#).

Note

If you enable the `clr_enabled` parameter on SQL Server 2017 or 2019, you can't use the common language runtime (CLR) on your DB instance. For more information, see [Features not supported and features with limited support \(p. 1071\)](#).

- The following control flow tasks are supported:
 - Analysis Services Execute DDL Task
 - Analysis Services Processing Task
 - Bulk Insert Task
 - Check Database Integrity Task
 - Data Flow Task
 - Data Mining Query Task
 - Data Profiling Task
 - Execute Package Task
 - Execute SQL Server Agent Job Task
 - Execute SQL Task
 - Execute T-SQL Statement Task
 - Notify Operator Task
 - Rebuild Index Task
 - Reorganize Index Task
 - Shrink Database Task
 - Transfer Database Task
 - Transfer Jobs Task
 - Transfer Logins Task
 - Transfer SQL Server Objects Task
 - Update Statistics Task
- Only project deployment is supported.
- Running SSIS packages by using SQL Server Agent is supported.
- SSIS log records can be inserted only into user-created databases.
- Use only the D:\S3 folder for working with files. Files placed in any other directory are deleted. Be aware of a few other file location details:
 - Place SSIS project input and output files in the D:\S3 folder.
 - For the Data Flow Task, change the location for `BLOBTempStoragePath` and `BufferTempStoragePath` to a file inside the D:\S3 folder. The file path must start with D:\S3\.
 - Ensure that all parameters, variables, and expressions used for file connections point to the D:\S3 folder.
 - On Multi-AZ instances, files created by SSIS in the D:\S3 folder are deleted after a failover. For more information, see [Multi-AZ limitations for S3 integration \(p. 1165\)](#).
 - Upload the files created by SSIS in the D:\S3 folder to your Amazon S3 bucket to make them durable.
- Import Column and Export Column transformations and the Script component on the Data Flow Task aren't supported.
- You can't enable dump on running SSIS packages, and you can't add data taps on SSIS packages.
- The SSIS Scale Out feature isn't supported.
- You can't deploy projects directly. We provide RDS stored procedures to do this. For more information, see [Deploying an SSIS project \(p. 1259\)](#). 1252

- Build SSIS project (.ispac) files with the DoNotSavePasswords protection mode for deploying on RDS.
- SSIS isn't supported on Always On instances with read replicas.
- You can't back up the SSISDB database that is associated with the SSIS option.
- Importing and restoring the SSISDB database from other instances of SSIS isn't supported.
- You can connect to other SQL Server DB instances or to an Oracle data source. Connecting to other database engines, such as MySQL or PostgreSQL, isn't supported for SSIS on RDS for SQL Server. For more information on connecting to an Oracle data source, see [Linked Servers with Oracle OLEDB \(p. 1206\)](#).

Enabling SSIS

You enable SSIS by adding the SSIS option to your DB instance. Use the following process:

1. Create a new option group, or choose an existing option group.
2. Add the SSIS option to the option group.
3. Create a new parameter group, or choose an existing parameter group.
4. Modify the parameter group to set the `clr_enabled` parameter to 1.
5. Associate the option group and parameter group with the DB instance.
6. Enable Amazon S3 integration.

Note

If a database with the name SSISDB or a reserved SSIS login already exists on the DB instance, you can't enable SSIS on the instance.

Creating the option group for SSIS

To work with SSIS, create an option group or modify an option group that corresponds to the SQL Server edition and version of the DB instance that you plan to use. To do this, use the AWS Management Console or the AWS CLI.

Console

The following procedure creates an option group for SQL Server Standard Edition 2016.

To create the option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** window, do the following:
 - a. For **Name**, enter a name for the option group that is unique within your AWS account, such as **ssis-se-2016**. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, enter a brief description of the option group, such as **SSIS option group for SQL Server SE 2016**. The description is used for display purposes.
 - c. For **Engine**, choose **sqlserver-se**.
 - d. For **Major engine version**, choose **13.00**.
5. Choose **Create**.

CLI

The following procedure creates an option group for SQL Server Standard Edition 2016.

To create the option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-option-group \
    --option-group-name ssis-se-2016 \
    --engine-name sqlserver-se \
    --major-engine-version 13.00 \
    --option-group-description "SSIS option group for SQL Server SE 2016"
```

For Windows:

```
aws rds create-option-group ^
    --option-group-name ssis-se-2016 ^
    --engine-name sqlserver-se ^
    --major-engine-version 13.00 ^
    --option-group-description "SSIS option group for SQL Server SE 2016"
```

Adding the SSIS option to the option group

Next, use the AWS Management Console or the AWS CLI to add the SSIS option to your option group.

Console

To add the SSIS option

- Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
- In the navigation pane, choose **Option groups**.
- Choose the option group that you just created, **ssis-se-2016** in this example.
- Choose **Add option**.
- Under **Option details**, choose **SSIS** for **Option name**.
- Under **Scheduling**, choose whether to add the option immediately or at the next maintenance window.
- Choose **Add option**.

CLI

To add the SSIS option

- Add the SSIS option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
```

```
--option-group-name ssis-se-2016 \
--options OptionName=SSIS \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name ssis-se-2016 ^
--options OptionName=SSIS ^
--apply-immediately
```

Creating the parameter group for SSIS

Create or modify a parameter group for the `clr` enabled parameter that corresponds to the SQL Server edition and version of the DB instance that you plan to use for SSIS.

Console

The following procedure creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.
4. In the **Create parameter group** pane, do the following:
 - a. For **Parameter group family**, choose `sqlserver-se-13.0`.
 - b. For **Group name**, enter an identifier for the parameter group, such as `ssis-sqlserver-se-13`.
 - c. For **Description**, enter `clr enabled parameter group`.
5. Choose **Create**.

CLI

The following procedure creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
--db-parameter-group-name ssis-sqlserver-se-13 \
--db-parameter-group-family "sqlserver-se-13.0" \
--description "clr enabled parameter group"
```

For Windows:

```
aws rds create-db-parameter-group ^
```

```
--db-parameter-group-name ssis-sqlserver-se-13 ^
--db-parameter-group-family "sqlserver-se-13.0" ^
--description "clr enabled parameter group"
```

Modifying the parameter for SSIS

Modify the `clr enabled` parameter in the parameter group that corresponds to the SQL Server edition and version of your DB instance. For SSIS, set the `clr enabled` parameter to 1.

Console

The following procedure modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group, such as **ssis-sqlserver-se-13**.
4. Under **Parameters**, filter the parameter list for **clr**.
5. Choose **clr enabled**.
6. Choose **Edit parameters**.
7. From **Values**, choose **1**.
8. Choose **Save changes**.

CLI

The following procedure modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name ssis-sqlserver-se-13 \
  --parameters "ParameterName='clr enabled',ParameterValue=1,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name ssis-sqlserver-se-13 ^
  --parameters "ParameterName='clr enabled',ParameterValue=1,ApplyMethod=immediate"
```

Associating the option group and parameter group with your DB instance

To associate the SSIS option group and parameter group with your DB instance, use the AWS Management Console or the AWS CLI

Note

If you use an existing instance, it must already have an Active Directory domain and AWS Identity and Access Management (IAM) role associated with it. If you create a new instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

Console

To finish enabling SSIS, associate your SSIS option group and parameter group with a new or existing DB instance:

- For a new DB instance, associate them when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, associate them by modifying the instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

You can associate the SSIS option group and parameter group with a new or existing DB instance.

To create an instance with the SSIS option group and parameter group

- Specify the same DB engine type and major version as you used when creating the option group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier myssisinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 13.00.5426.0.v1 \
    --allocated-storage 100 \
    --master-user-password secret123 \
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name ssis-se-2016 \
    --db-parameter-group-name ssis-sqlserver-se-13
```

For Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier myssisinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 13.00.5426.0.v1 ^
    --allocated-storage 100 ^
    --master-user-password secret123 ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name ssis-se-2016 ^
    --db-parameter-group-name ssis-sqlserver-se-13
```

To modify an instance and associate the SSIS option group and parameter group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier myssisinstance \
--option-group-name ssis-se-2016 \
--db-parameter-group-name ssis-sqlserver-se-13 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier myssisinstance ^
--option-group-name ssis-se-2016 ^
--db-parameter-group-name ssis-sqlserver-se-13 ^
--apply-immediately
```

Enabling S3 integration

To download SSIS project (.ispac) files to your host for deployment, use S3 file integration. For more information, see [Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 \(p. 1153\)](#).

Administrative permissions on SSISDB

When the instance is created or modified with the SSIS option, the result is an SSISDB database with the ssis_admin and ssis_logreader roles granted to the master user. The master user has the following privileges in SSISDB:

- alter on ssis_admin role
- alter on ssis_logreader role
- alter any user

Because the master user is a SQL-authenticated user, you can't use the master user for executing SSIS packages. The master user can use these privileges to create new SSISDB users and add them to the ssis_admin and ssis_logreader roles. Doing this is useful for giving access to your domain users for using SSIS.

Setting up a Windows-authenticated user for SSIS

The master user can use the following code example to set up a Windows-authenticated login in SSISDB and grant the required procedure permissions. Doing this grants permissions to the domain user to deploy and run SSIS packages, use S3 file transfer procedures, create credentials, and work with the SQL Server Agent proxy. For more information, see [Credentials \(database engine\)](#) and [Create a SQL Server Agent proxy](#) in the Microsoft documentation.

Note

You can grant some or all of the following permissions as needed to Windows-authenticated users.

Example

```

USE [SSISDB]
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]
ALTER ROLE [ssis_admin] ADD MEMBER [mydomain\user_name]
ALTER ROLE [ssis_logreader] ADD MEMBER [mydomain\user_name]
GO

USE [msdb]
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]
GRANT EXEC ON msdb.dbo.rds_msbi_task TO [mydomain\user_name] with grant option
GRANT SELECT ON msdb.dbo.rds_fn_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_cancel_task TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_download_from_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_upload_to_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_delete_from_filesystem TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_gather_file_details TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_add_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_update_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_grant_login_to_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_revoke_login_from_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_delete_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_login_for_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_proxy_for_subsystem TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_sqlagent_proxy TO [mydomain\user_name] WITH GRANT OPTION
ALTER ROLE [SQLAgentUserRole] ADD MEMBER [mydomain\user_name]
GO

USE [master]
GO
GRANT ALTER ANY CREDENTIAL TO [mydomain\user_name]
GO

```

Deploying an SSIS project

On RDS, you can't deploy SSIS projects directly by using SQL Server Management Studio (SSMS) or SSIS procedures. To download project files from Amazon S3 and then deploy them, use RDS stored procedures.

To run the stored procedures, log in as any user that you granted permissions for running the stored procedures. For more information, see [Setting up a Windows-authenticated user for SSIS \(p. 1258\)](#).

To deploy the SSIS project

1. Download the project (.ispac) file.

```

exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/ssisproject.ispac',
[@rds_file_path='D:\S3\ssisproject.ispac'],
[@overwrite_file=1];

```

2. Submit the deployment task, making sure of the following:

- The folder is present in the SSIS catalog.
- The project name matches the project name that you used while developing the SSIS project.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSIS_DEPLOY_PROJECT',
@folder_name='DEMO',
@project_name='ssisproject',
@file_path='D:\S3\ssisproject.ispac';
```

Monitoring the status of a deployment task

To track the status of your deployment task, call the `rds_fn_task_status` function. It takes two parameters. The first parameter should always be `NULL` because it doesn't apply to SSIS. The second parameter accepts a task ID.

To see a list of all tasks, set the first parameter to `NULL` and the second parameter to `0`, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

To get a specific task, set the first parameter to `NULL` and the second parameter to the task ID, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

The `rds_fn_task_status` function returns the following information.

Output parameter	Description
<code>task_id</code>	The ID of the task.
<code>task_type</code>	<code>SSIS_DEPLOY_PROJECT</code>
<code>database_name</code>	Not applicable to SSIS tasks.
<code>% complete</code>	The progress of the task as a percentage.
<code>duration (mins)</code>	The amount of time spent on the task, in minutes.
<code>lifecycle</code>	The status of the task. Possible statuses are the following: <ul style="list-style-type: none">• <code>CREATED</code> – After you call the <code>msdb.dbo.rds_msbi_task</code> stored procedure, a task is created and the status is set to <code>CREATED</code>.• <code>IN_PROGRESS</code> – After a task starts, the status is set to <code>IN_PROGRESS</code>. It can take up to five minutes for the status to change from <code>CREATED</code> to <code>IN_PROGRESS</code>.• <code>SUCCESS</code> – After a task completes, the status is set to <code>SUCCESS</code>.• <code>ERROR</code> – If a task fails, the status is set to <code>ERROR</code>. For more information about the error, see the <code>task_info</code> column.

Output parameter	Description
	<ul style="list-style-type: none"> CANCEL_REQUESTED – After you call <code>rds_cancel_task</code>, the status of the task is set to CANCEL_REQUESTED. CANCELLED – After a task is successfully canceled, the status of the task is set to CANCELLED.
<code>task_info</code>	Additional information about the task. If an error occurs during processing, this column contains information about the error.
<code>last_updated</code>	The date and time that the task status was last updated.
<code>created_at</code>	The date and time that the task was created.
<code>S3_object_arn</code>	Not applicable to SSIS tasks.
<code>overwrite_S3_backup_file</code>	Not applicable to SSIS tasks.
<code>KMS_master_key_arn</code>	Not applicable to SSIS tasks.
<code>filepath</code>	Not applicable to SSIS tasks.
<code>overwrite_file</code>	Not applicable to SSIS tasks.
<code>task_metadata</code>	Metadata associated with the SSIS task.

Using SSIS

After deploying the SSIS project into the SSIS catalog, you can run packages directly from SSMS or schedule them by using SQL Server Agent. You must use a Windows-authenticated login for executing SSIS packages. For more information, see [Setting up a Windows-authenticated user for SSIS \(p. 1258\)](#).

Topics

- [Setting database connection managers for SSIS projects \(p. 1261\)](#)
- [Creating an SSIS proxy \(p. 1262\)](#)
- [Scheduling an SSIS package using SQL Server Agent \(p. 1263\)](#)
- [Revoking SSIS access from the proxy \(p. 1263\)](#)

Setting database connection managers for SSIS projects

When you use a connection manager, you can use these types of authentication:

- For local database connections, you can use SQL authentication or Windows authentication. For Windows authentication, use `DB_instance_name.fully_qualified_domain_name` as the server name of the connection string.

An example is `myssisisinstance.corp-ad.example.com`, where `myssisisinstance` is the DB instance name and `corp-ad.example.com` is the fully qualified domain name.

- For remote connections, always use SQL authentication.

Creating an SSIS proxy

To be able to schedule SSIS packages using SQL Server Agent, create an SSIS credential and an SSIS proxy. Run these procedures as a Windows-authenticated user.

To create the SSIS credential

- Create the credential for the proxy. To do this, you can use SSMS or the following SQL statement.

```
USE [master]
GO
CREATE CREDENTIAL [SSIS_Credential] WITH IDENTITY = N'mydomain\user_name', SECRET =
N'mysecret'
GO
```

Note

IDENTITY must be a domain-authenticated login. Replace *mysecret* with the password for the domain-authenticated login.

Whenever the SSISDB primary host is changed, alter the SSIS proxy credentials to allow the new host to access them.

To create the SSIS proxy

1. Use the following SQL statement to create the proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_add_proxy
    @proxy_name=N'SSIS_Proxy',@credential_name=N'SSIS_Credential',@description=N''
GO
```

2. Use the following SQL statement to grant access to the proxy to other users.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_grant_login_to_proxy
    @proxy_name=N'SSIS_Proxy',@login_name=N'mydomain\user_name'
GO
```

3. Use the following SQL statement to give the SSIS subsystem access to the proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
    @task_type='GRANT_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

To view the proxy and grants on the proxy

1. Use the following SQL statement to view the grantees of the proxy.

```
USE [msdb]
GO
EXEC sp_help_proxy
GO
```

2. Use the following SQL statement to view the subsystem grants.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_enum_proxy_for_subsystem
GO
```

Scheduling an SSIS package using SQL Server Agent

After you create the credential and proxy and grant SSIS access to the proxy, you can create a SQL Server Agent job to schedule the SSIS package.

To schedule the SSIS package

- You can use SSMS or T-SQL for creating the SQL Server Agent job. The following example uses T-SQL.

```
USE [msdb]
GO
DECLARE @jobId BINARY(16)
EXEC msdb.dbo.sp_add_job @job_name=N'MYSSISJob',
@enabled=1,
@notify_level_eventlog=0,
@notify_level_email=2,
@notify_level_page=2,
@delete_level=0,
@category_name=N'[Uncategorized (Local)]',
@job_id = @jobId OUTPUT
GO
EXEC msdb.dbo.sp_add_jobobserver @job_name=N'MYSSISJob',@server_name=N'(local)'
GO
EXEC msdb.dbo.sp_add_jobstep @job_name=N'MYSSISJob',@step_name=N'ExecuteSSISPackage',
@step_id=1,
@cmdexec_success_code=0,
@on_success_action=1,
@on_fail_action=2,
@retry_attempts=0,
@retry_interval=0,
@os_run_priority=0,
@subsystem=N'SSIS',
@command=N'/ISSERVER "\"\\SSISDB\MySSISFolder\MySSISProject\MySSISPackage.dtsx\""
 SERVER \"\\my-rds-ssis-instance.corp-ad.company.com\\\""
 /Par '\"$ServerOption::LOGGING_LEVEL(Int16)\";1 /Par
 '\"$ServerOption::SYNCHRONIZED(Boolean)\"';True /CALLERINFO SQLAGENT /REPORTING E',
@database_name=N'master',
@flags=0,
@proxy_name=N'SSIS_Proxy'
GO
```

Revoking SSIS access from the proxy

You can revoke access to the SSIS subsystem and delete the SSIS proxy using the following stored procedures.

To revoke access and delete the proxy

1. Revoke subsystem access.

```
USE [msdb]
GO
```

```
EXEC msdb.dbo.rds_sqlagent_proxy
    @task_type='REVOKE_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

2. Revoke the grants on the proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_revoke_login_from_proxy
    @proxy_name=N'SSIS_Proxy',@name=N'mydomain\user_name'
GO
```

3. Delete the proxy.

```
USE [msdb]
GO
EXEC dbo.sp_delete_proxy @proxy_name = N'SSIS_Proxy'
GO
```

Disabling SSIS

To disable SSIS, remove the SSIS option from its option group.

Important

Removing the option doesn't delete the SSISDB database, so you can safely remove the option without losing the SSIS projects.

You can re-enable the SSIS option after removal to reuse the SSIS projects that were previously deployed to the SSIS catalog.

Console

The following procedure removes the SSIS option.

To remove the SSIS option from its option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the SSIS option (ssis-se-2016 in the previous examples).
4. Choose **Delete option**.
5. Under **Deletion options**, choose **SSIS** for **Options to delete**.
6. Under **Apply immediately**, choose **Yes** to delete the option immediately, or **No** to delete it at the next maintenance window.
7. Choose **Delete**.

CLI

The following procedure removes the SSIS option.

To remove the SSIS option from its option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
--option-group-name ssis-se-2016 \
--options SSIS \
--apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
--option-group-name ssis-se-2016 ^
--options SSIS ^
--apply-immediately
```

Dropping the SSISDB database

After removing the SSIS option, the SSISDB database isn't deleted. To drop the SSISDB database, use the `rds_drop_ssis_database` stored procedure after removing the SSIS option.

To drop the SSIS database

- Use the following stored procedure.

```
USE [msdb]
GO
EXEC dbo.rds_drop_ssis_database
GO
```

After dropping the SSISDB database, if you re-enable the SSIS option you get a fresh SSISDB catalog.

Support for SQL Server Reporting Services in Amazon RDS for SQL Server

Microsoft SQL Server Reporting Services (SSRS) is a server-based application used for report generation and distribution. It's part of a suite of SQL Server services that also includes SQL Server Analysis Services (SSAS) and SQL Server Integration Services (SSIS). SSRS is a service built on top of SQL Server. You can use it to collect data from various data sources and present it in a way that's easily understandable and ready for analysis.

Amazon RDS for SQL Server supports running SSRS directly on RDS DB instances. You can use SSRS with existing or new DB instances.

RDS supports SSRS for SQL Server Standard and Enterprise Editions on the following versions:

- SQL Server 2019, version 15.00.4043.16.v1 and higher
- SQL Server 2017, version 14.00.3223.3.v1 and higher
- SQL Server 2016, version 13.00.5820.21.v1 and higher

Contents

- [Limitations and recommendations \(p. 1266\)](#)
- [Turning on SSRS \(p. 1267\)](#)
 - [Creating an option group for SSRS \(p. 1267\)](#)
 - [Adding the SSRS option to your option group \(p. 1268\)](#)
 - [Associating your option group with your DB instance \(p. 1270\)](#)
 - [Allowing inbound access to your VPC security group \(p. 1272\)](#)
- [Report server databases \(p. 1272\)](#)
- [SSRS log files \(p. 1272\)](#)
- [Accessing the SSRS web portal \(p. 1272\)](#)
 - [Using SSL on RDS \(p. 1272\)](#)
 - [Granting access to domain users \(p. 1272\)](#)
 - [Accessing the web portal \(p. 1272\)](#)
- [Deploying reports to SSRS \(p. 1273\)](#)
- [Using SSRS Email to send reports \(p. 1274\)](#)
- [Revoking system-level permissions \(p. 1275\)](#)
- [Monitoring the status of a task \(p. 1275\)](#)
- [Turning off SSRS \(p. 1277\)](#)
- [Deleting the SSRS databases \(p. 1277\)](#)

Limitations and recommendations

The following limitations and recommendations apply to running SSRS on RDS for SQL Server:

- You can't use SSRS on DB instances that have read replicas.
- Instances must use AWS Managed Microsoft AD for SSRS web portal and web server authentication.
- Importing and restoring report server databases from other instances of SSRS isn't supported.

Make sure to use the databases that are created when the SSRS option is added to the RDS DB instance. For more information, see [Report server databases \(p. 1272\)](#).

- You can't configure SSRS to listen on the default SSL port (443). The allowed values are 1150–49511, except 1234, 1434, 3260, 3343, 3389, and 47001.
- Subscriptions through a Microsoft Windows file share aren't supported.
- Using Reporting Services Configuration Manager isn't supported.
- Creating and modifying roles isn't supported.
- Modifying report server properties isn't supported.
- System administrator and system user roles aren't granted.
- You can't edit system-level role assignments through the web portal.

Turning on SSRS

Use the following process to turn on SSRS for your DB instance:

1. Create a new option group, or choose an existing option group.
2. Add the SSRS option to the option group.
3. Associate the option group with the DB instance.
4. Allow inbound access to the virtual private cloud (VPC) security group for the SSRS listener port.

Creating an option group for SSRS

To work with SSRS, create an option group that corresponds to the SQL Server engine and version of the DB instance that you plan to use. To do this, use the AWS Management Console or the AWS CLI.

Note

You can also use an existing option group if it's for the correct SQL Server engine and version.

Console

The following procedure creates an option group for SQL Server Standard Edition 2017.

To create the option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** pane, do the following:
 - a. For **Name**, enter a name for the option group that is unique within your AWS account, such as **ssrs-se-2017**. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, enter a brief description of the option group, such as **SSRS option group for SQL Server SE 2017**. The description is used for display purposes.
 - c. For **Engine**, choose **sqlserver-se**.
 - d. For **Major engine version**, choose **14.00**.
5. Choose **Create**.

CLI

The following procedure creates an option group for SQL Server Standard Edition 2017.

To create the option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-option-group \
--option-group-name ssrs-se-2017 \
--engine-name sqlserver-se \
--major-engine-version 14.00 \
--option-group-description "SSRS option group for SQL Server SE 2017"
```

For Windows:

```
aws rds create-option-group ^
--option-group-name ssrs-se-2017 ^
--engine-name sqlserver-se ^
--major-engine-version 14.00 ^
--option-group-description "SSRS option group for SQL Server SE 2017"
```

Adding the SSRS option to your option group

Next, use the AWS Management Console or the AWS CLI to add the SSRS option to your option group.

Console

To add the SSRS option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group that you just created, then choose **Add option**.
4. Under **Option details**, choose **SSRS** for **Option name**.
5. Under **Option settings**, do the following:
 - a. Enter the port for the SSRS service to listen on. The default is 8443. For a list of allowed values, see [Limitations and recommendations \(p. 1266\)](#).
 - b. Enter a value for **Max memory**.

Max memory specifies the upper threshold above which no new memory allocation requests are granted to report server applications. The number is a percentage of the total memory of the DB instance. The allowed values are 10–80.
6. To use SSRS Email to send reports, choose the **Configure email delivery options** check box under **Email delivery in reporting services**, and then do the following:
 - a. For **Sender email address**, enter the email address to use in the **From** field of messages sent by SSRS Email.

Specify a user account that has permission to send mail from the SMTP server.
 - b. For **SMTP server**, specify the SMTP server or gateway to use.

It can be an IP address, the NetBIOS name of a computer on your corporate intranet, or a fully qualified domain name.
 - c. For **SMTP port**, enter the port to use to connect to the mail server. The default is 25.
 - d. To use authentication:
 - i. Select the **Use authentication** check box.

- ii. For **Secret Amazon Resource Name (ARN)** enter the AWS Secrets Manager ARN for the user credentials.

Use the following format:

arn:aws:secretsmanager:Region:AccountId:secret:SecretName-6RandomCharacters

For example:

arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3

For more information on creating the secret, see [Using SSRS Email to send reports \(p. 1274\)](#).

- e. Select the **Use Secure Sockets Layer (SSL)** check box to encrypt email messages using SSL.
7. Under **Scheduling**, choose whether to add the option immediately or at the next maintenance window.
8. Choose **Add option**.

CLI

To add the SSRS option

1. Create a JSON file, for example `ssrs-option.json`.
 - a. Set the following required parameters:
 - OptionGroupName – The name of option group that you created or chose previously (`ssrs-se-2017` in the following example).
 - Port – The port for the SSRS service to listen on. The default is 8443. For a list of allowed values, see [Limitations and recommendations \(p. 1266\)](#).
 - VpcSecurityGroupMemberships – VPC security group memberships for your RDS DB instance.
 - MAX_MEMORY – The upper threshold above which no new memory allocation requests are granted to report server applications. The number is a percentage of the total memory of the DB instance. The allowed values are 10–80.
 - b. (Optional) Set the following parameters to use SSRS Email:
 - SMTP_ENABLE_EMAIL – Set to `true` to use SSRS Email. The default is `false`.
 - SMTP_SENDER_EMAIL_ADDRESS – The email address to use in the **From** field of messages sent by SSRS Email. Specify a user account that has permission to send mail from the SMTP server.
 - SMTP_SERVER – The SMTP server or gateway to use. It can be an IP address, the NetBIOS name of a computer on your corporate intranet, or a fully qualified domain name.
 - SMTP_PORT – The port to use to connect to the mail server. The default is 25.
 - SMTP_USE_SSL – Set to `true` to encrypt email messages using SSL. The default is `true`.
 - SMTP_EMAIL_CREDENTIALS_SECRET_ARN – The Secrets Manager ARN that holds the user credentials. Use the following format:

arn:aws:secretsmanager:Region:AccountId:secret:SecretName-6RandomCharacters

For more information on creating the secret, see [Using SSRS Email to send reports \(p. 1274\)](#).

- SMTP_USE_ANONYMOUS_AUTHENTICATION – Set to `true` and don't include `SMTP_EMAIL_CREDENTIALS_SECRET_ARN` if you don't want to use authentication.

The default is `false` when `SMTP_ENABLE_EMAIL` is `true`.

The following example includes the SSRS Email parameters, using the secret ARN.

```
{  
    "OptionGroupName": "ssrs-se-2017",  
    "OptionsToInclude": [  
        {  
            "OptionName": "SSRS",  
            "Port": 8443,  
            "VpcSecurityGroupMemberships": ["sg-0abcdef123"],  
            "OptionSettings": [  
                {"Name": "MAX_MEMORY", "Value": "60"},  
                {"Name": "SMTP_ENABLE_EMAIL", "Value": "true"},  
                {"Name": "SMTP_SENDER_EMAIL_ADDRESS", "Value": "nobody@example.com"},  
                {"Name": "SMTP_SERVER", "Value": "email-smtp.us-west-2.amazonaws.com"},  
                {"Name": "SMTP_PORT", "Value": "25"},  
                {"Name": "SMTP_USE_SSL", "Value": "true"},  
                {"Name": "SMTP_EMAIL_CREDENTIALS_SECRET_ARN", "Value": "  
arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3"}  
            ]  
        }  
    ],  
    "ApplyImmediately": true  
}
```

2. Add the SSRS option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \  
    --cli-input-json file://ssrs-option.json \  
    --apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^  
    --cli-input-json file://ssrs-option.json ^  
    --apply-immediately
```

Associating your option group with your DB instance

Use the AWS Management Console or the AWS CLI to associate your option group with your DB instance.

If you use an existing DB instance, it must already have an Active Directory domain and AWS Identity and Access Management (IAM) role associated with it. If you create a new instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

Console

You can associate your option group with a new or existing DB instance:

- For a new DB instance, associate the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, modify the instance and associate the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

CLI

You can associate your option group with a new or existing DB instance.

To create a DB instance that uses your option group

- Specify the same DB engine type and major version as you used when creating the option group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
    --db-instance-identifier myssrsinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 14.00.3223.3.v1 \
    --allocated-storage 100 \
    --master-user-password secret123 \
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name ssrs-se-2017
```

For Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier myssrsinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 14.00.3223.3.v1 ^
    --allocated-storage 100 ^
    --master-user-password secret123 ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name ssrs-se-2017
```

To modify a DB instance to use your option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier myssrsinstance \
    --option-group-name ssrs-se-2017 \
    --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier myssrsinstance ^
```

```
--option-group-name ssrs-se-2017 ^
--apply-immediately
```

Allowing inbound access to your VPC security group

To allow inbound access to the VPC security group associated with your DB instance, create an inbound rule for the specified SSRS listener port. For more information about setting up security groups, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

Report server databases

When your DB instance is associated with the SSRS option, two new databases are created on your DB instance: rdsadmin_ReportServer and rdsadmin_ReportServerTempDB. These databases act as the ReportServer and ReportServerTempDB databases. SSRS stores its data in the ReportServer database and caches its data in the ReportServerTempDB database.

RDS owns and manages these databases, so database operations on them such as ALTER and DROP aren't permitted. However, you can perform read operations on the rdsadmin_ReportServer database.

SSRS log files

You can access ReportServerService_*timestamp*.log files. These report server logs can be found in the D:\rdsdbdata\Log\SSRS directory. (The D:\rdsdbdata\Log directory is also the parent directory for error logs and SQL Server Agent logs.)

For existing SSRS instances, restarting the SSRS service might be necessary to access report server logs. You can restart the service by updating the SSRS option.

For more information, see [Working with Microsoft SQL Server logs \(p. 1308\)](#).

Accessing the SSRS web portal

Use the following process to access the SSRS web portal:

1. Turn on Secure Sockets Layer (SSL).
2. Grant access to domain users.
3. Access the web portal using a browser and the domain user credentials.

Using SSL on RDS

SSRS uses the HTTPS SSL protocol for its connections. To work with this protocol, import an SSL certificate into the Microsoft Windows operating system on your client computer.

For more information on SSL certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For more information about using SSL with SQL Server, see [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#).

Granting access to domain users

In a new SSRS activation, there are no role assignments in SSRS. To give a domain user or user group access to the web portal, RDS provides a stored procedure.

To grant access to a domain user on the web portal

- Use the following stored procedure.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSRS_GRANT_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';
```

The domain user or user group is granted the RDS_SSRS_ROLE system role. This role has the following system-level tasks granted to it:

- Run reports
- Manage jobs
- Manage shared schedules
- View shared schedules

The item-level role of Content Manager on the root folder is also granted.

Accessing the web portal

After the SSRS_GRANT_PORTAL_PERMISSION task finishes successfully, you have access to the portal using a web browser. The web portal URL has the following format.

```
https://rds_endpoint:port/Reports
```

In this format, the following applies:

- *rds_endpoint* – The endpoint for the RDS DB instance that you're using with SSRS.

You can find the endpoint on the **Connectivity & security** tab for your DB instance. For more information, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#).

- *port* – The listener port for SSRS that you set in the SSRS option.

To access the web portal

1. Enter the web portal URL in your browser.

```
https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/Reports
```

2. Log in with the credentials for a domain user that you granted access with the SSRS_GRANT_PORTAL_PERMISSION task.

Deploying reports to SSRS

After you have access to the web portal, you can deploy reports to it. You can use the Upload tool in the web portal to upload reports, or deploy directly from [SQL Server data tools \(SSDT\)](#). When deploying from SSDT, ensure the following:

- The user who launched SSDT has access to the SSRS web portal.
- The TargetServerURL value in the SSRS project properties is set to the HTTPS endpoint of the RDS DB instance suffixed with ReportServer, for example:

```
https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/ReportServer
```

Using SSRS Email to send reports

SSRS includes the SSRS Email extension, which you can use to send reports to users.

To configure SSRS Email, use the SSRS option settings. For more information, see [Adding the SSRS option to your option group \(p. 1268\)](#).

After configuring SSRS Email, you can subscribe to reports on the report server. For more information, see [Email delivery in Reporting Services](#) in the Microsoft documentation.

Integration with AWS Secrets Manager is required for SSRS Email to function on RDS. To integrate with Secrets Manager, you create a secret.

Note

If you change the secret later, you also have to update the SSRS option in the option group.

To create a secret for SSRS Email

1. Follow the steps in [Create a secret](#) in the *AWS Secrets Manager User Guide*.
 - a. For **Select secret type**, choose **Other type of secrets**.
 - b. For **Key/value pairs**, enter the following:
 - **SMTP_USERNAME** – Enter a user with permission to send mail from the SMTP server.
 - **SMTP_PASSWORD** – Enter a password for the SMTP user.
 - c. For **Encryption key**, don't use the default AWS KMS key. Use your own existing key, or create a new one.

The KMS key policy must allow the kms:Decrypt action, for example:

```
{  
    "Sid": "Allow use of the key",  
    "Effect": "Allow",  
    "Principal": {  
        "Service": [  
            "rds.amazonaws.com"  
        ]  
    },  
    "Action": [  
        "kms:Decrypt"  
    ],  
    "Resource": "*"  
}
```

2. Follow the steps in [Attach a permissions policy to a secret](#) in the *AWS Secrets Manager User Guide*. The permissions policy gives the secretsmanager:GetSecretValue action to the rds.amazonaws.com service principal.

We recommend that you use the aws:sourceAccount and aws:sourceArn conditions in the policy to avoid the *confused deputy* problem. Use your AWS account for aws:sourceAccount and the option group ARN for aws:sourceArn. For more information, see [Preventing cross-service confused deputy problems \(p. 2046\)](#).

The following example shows a permissions policy.

```
{  
    "Version" : "2012-10-17",  
    "Statement" : [ {  
        "Effect" : "Allow",  
        "Principal" : {
```

```

        "Service" : "rds.amazonaws.com"
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "aws:sourceAccount" : "123456789012"
        },
        "ArnLike" : {
            "aws:sourceArn" : "arn:aws:rds:us-west-2:123456789012:og:ssrs-se-2017"
        }
    }
}
]
}

```

For more examples, see [Permissions policy examples](#) in the *AWS Secrets Manager User Guide*.

Revoking system-level permissions

The RDS_SSRS_ROLE system role doesn't have sufficient permissions to delete system-level role assignments. To remove a user or user group from RDS_SSRS_ROLE, use the same stored procedure that you used to grant the role but use the SSRS_REVOKER_PORTAL_PERMISSION task type.

To revoke access from a domain user for the web portal

- Use the following stored procedure.

```

exec msdb.dbo.rds_msbi_task
@task_type='SSRS_REVOKER_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';

```

Doing this deletes the user from the RDS_SSRS_ROLE system role. It also deletes the user from the Content Manager item-level role if the user has it.

Monitoring the status of a task

To track the status of your granting or revoking task, call the rds_fn_task_status function. It takes two parameters. The first parameter should always be NULL because it doesn't apply to SSRS. The second parameter accepts a task ID.

To see a list of all tasks, set the first parameter to NULL and the second parameter to 0, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

To get a specific task, set the first parameter to NULL and the second parameter to the task ID, as shown in the following example.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

The rds_fn_task_status function returns the following information.

Output parameter	Description
task_id	The ID of the task.

Output parameter	Description
task_type	For SSRS, tasks can have the following task types: <ul style="list-style-type: none"> • SSRS_GRANT_PORTAL_PERMISSION • SSRS_REVOKER_PORTAL_PERMISSION
database_name	Not applicable to SSRS tasks.
% complete	The progress of the task as a percentage.
duration (mins)	The amount of time spent on the task, in minutes.
lifecycle	The status of the task. Possible statuses are the following: <ul style="list-style-type: none"> • CREATED – After you call one of the SSRS stored procedures, a task is created and the status is set to CREATED. • IN_PROGRESS – After a task starts, the status is set to IN_PROGRESS. It can take up to five minutes for the status to change from CREATED to IN_PROGRESS. • SUCCESS – After a task completes, the status is set to SUCCESS. • ERROR – If a task fails, the status is set to ERROR. For more information about the error, see the task_info column. • CANCEL_REQUESTED – After you call the rds_cancel_task stored procedure, the status of the task is set to CANCEL_REQUESTED. • CANCELLED – After a task is successfully canceled, the status of the task is set to CANCELLED.
task_info	Additional information about the task. If an error occurs during processing, this column contains information about the error.
last_updated	The date and time that the task status was last updated.
created_at	The date and time that the task was created.
S3_object_arn	Not applicable to SSRS tasks.
overwrite_S3_backup_file	Not applicable to SSRS tasks.
KMS_master_key_arn	Not applicable to SSRS tasks.
filepath	Not applicable to SSRS tasks.
overwrite_file	Not applicable to SSRS tasks.
task_metadata	Metadata associated with the SSRS task.

Turning off SSRS

To turn off SSRS, remove the SSRS option from its option group. Removing the option doesn't delete the SSRS databases. For more information, see [Deleting the SSRS databases \(p. 1277\)](#).

You can turn SSRS on again by adding back the SSRS option. If you have also deleted the SSRS databases, readding the option on the same DB instance creates new report server databases.

Console

To remove the SSRS option from its option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the SSRS option (`ssrs-se-2017` in the previous examples).
4. Choose **Delete option**.
5. Under **Deletion options**, choose **SSRS for Options to delete**.
6. Under **Apply immediately**, choose **Yes** to delete the option immediately, or **No** to delete it at the next maintenance window.
7. Choose **Delete**.

CLI

To remove the SSRS option from its option group

- Run one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
--option-group-name ssrs-se-2017 \
--options SSRS \
--apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
--option-group-name ssrs-se-2017 ^
--options SSRS ^
--apply-immediately
```

Deleting the SSRS databases

Removing the SSRS option doesn't delete the report server databases. To delete them, use the following stored procedure.

To delete the report server databases, be sure to remove the SSRS option first.

To delete the SSRS databases

- Use the following stored procedure.

```
exec msdb.dbo.rds_drop_ssrs_databases
```

Support for Microsoft Distributed Transaction Coordinator in RDS for SQL Server

A *distributed transaction* is a database transaction in which two or more network hosts are involved. RDS for SQL Server supports distributed transactions among hosts, where a single host can be one of the following:

- RDS for SQL Server DB instance
- On-premises SQL Server host
- Amazon EC2 host with SQL Server installed
- Any other EC2 host or RDS DB instance with a database engine that supports distributed transactions

In RDS, starting with SQL Server 2012 (version 11.00.5058.0.v1 and later), all editions of RDS for SQL Server support distributed transactions. The support is provided using Microsoft Distributed Transaction Coordinator (MSDTC). For in-depth information about MSDTC, see [Distributed Transaction Coordinator](#) in the Microsoft documentation.

Contents

- [Limitations \(p. 1279\)](#)
- [Enabling MSDTC \(p. 1280\)](#)
 - [Creating the option group for MSDTC \(p. 1280\)](#)
 - [Adding the MSDTC option to the option group \(p. 1281\)](#)
 - [Creating the parameter group for MSDTC \(p. 1283\)](#)
 - [Modifying the parameter for MSDTC \(p. 1283\)](#)
 - [Associating the option group and parameter group with the DB instance \(p. 1284\)](#)
- [Using distributed transactions \(p. 1286\)](#)
- [Using XA transactions \(p. 1286\)](#)
- [Using transaction tracing \(p. 1287\)](#)
- [Modifying the MSDTC option \(p. 1288\)](#)
- [Disabling MSDTC \(p. 1288\)](#)
- [Troubleshooting MSDTC for RDS for SQL Server \(p. 1289\)](#)

Limitations

The following limitations apply to using MSDTC on RDS for SQL Server:

- MSDTC isn't supported on instances using SQL Server Database Mirroring. For more information, see [Transactions - availability groups and database mirroring](#).
- The `in-doubt xact resolution` parameter must be set to 1 or 2. For more information, see [Modifying the parameter for MSDTC \(p. 1283\)](#).
- MSDTC requires all hosts participating in distributed transactions to be resolvable using their host names. RDS automatically maintains this functionality for domain-joined instances. However, for standalone instances make sure to configure the DNS server manually.
- Java Database Connectivity (JDBC) XA transactions are supported for SQL Server 2017 version 14.00.3223.3 and higher, and SQL Server 2019.
- Distributed transactions that depend on client dynamic link libraries (DLLs) on RDS instances aren't supported.
- Using custom XA dynamic link libraries isn't supported.

Enabling MSDTC

Use the following process to enable MSDTC for your DB instance:

1. Create a new option group, or choose an existing option group.
2. Add the MSDTC option to the option group.
3. Create a new parameter group, or choose an existing parameter group.
4. Modify the parameter group to set the `in-doubt xact resolution` parameter to 1 or 2.
5. Associate the option group and parameter group with the DB instance.

Creating the option group for MSDTC

Use the AWS Management Console or the AWS CLI to create an option group that corresponds to the SQL Server engine and version of your DB instance.

Note

You can also use an existing option group if it's for the correct SQL Server engine and version.

Console

The following procedure creates an option group for SQL Server Standard Edition 2016.

To create the option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose **Create group**.
4. In the **Create option group** pane, do the following:
 - a. For **Name**, enter a name for the option group that is unique within your AWS account, such as `msdtc-se-2016`. The name can contain only letters, digits, and hyphens.
 - b. For **Description**, enter a brief description of the option group, such as `MSDTC option group for SQL Server SE 2016`. The description is used for display purposes.
 - c. For **Engine**, choose `sqlserver-se`.
 - d. For **Major engine version**, choose `13.00`.
5. Choose **Create**.

CLI

The following example creates an option group for SQL Server Standard Edition 2016.

To create the option group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-option-group \
--option-group-name msdtc-se-2016 \
--engine-name sqlserver-se \
--major-engine-version 13.00 \
```

```
--option-group-description "MSDTC option group for SQL Server SE 2016"
```

For Windows:

```
aws rds create-option-group ^
--option-group-name msdtc-se-2016 ^
--engine-name sqlserver-se ^
--major-engine-version 13.00 ^
--option-group-description "MSDTC option group for SQL Server SE 2016"
```

Adding the MSDTC option to the option group

Next, use the AWS Management Console or the AWS CLI to add the MSDTC option to the option group.

The following option settings are required:

- **Port** – The port that you use to access MSDTC. Allowed values are 1150–49151 except for 1234, 1434, 3260, 3343, 3389, and 47001. The default value is 5000.

Make sure that the port you want to use is enabled in your firewall rules. Also, make sure as needed that this port is enabled in the inbound and outbound rules for the security group associated with your DB instance. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

- **Security groups** – The VPC security group memberships for your RDS DB instance.
- **Authentication type** – The authentication mode between hosts. The following authentication types are supported:
 - Mutual – The RDS instances are mutually authenticated to each other using integrated authentication. If this option is selected, all instances associated with this option group must be domain-joined.
 - None – No authentication is performed between hosts. We don't recommend using this mode in production environments.
- **Transaction log size** – The size of the MSDTC transaction log. Allowed values are 4–1024 MB. The default size is 4 MB.

The following option settings are optional:

- **Enable inbound connections** – Whether to allow inbound MSDTC connections to instances associated with this option group.
- **Enable outbound connections** – Whether to allow outbound MSDTC connections from instances associated with this option group.
- **Enable XA** – Whether to allow XA transactions. For more information on the XA protocol, see [XA specification](#).
- **Enable SNA LU** – Whether to allow the SNA LU protocol to be used for distributed transactions. For more information on SNA LU protocol support, see [Managing IBM CICS LU 6.2 transactions](#) in the Microsoft documentation.

Console

To add the MSDTC option

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group that you just created.

4. Choose **Add option**.
5. Under **Option details**, choose **MSDTC** for **Option name**.
6. Under **Option settings**:
 - a. For **Port**, enter the port number for accessing MSDTC. The default is **5000**.
 - b. For **Security groups**, choose the VPC security group to associate with the option.
 - c. For **Authentication type**, choose **Mutual** or **None**.
 - d. For **Transaction log size**, enter a value from 4–1024. The default is **4**.
7. Under **Additional configuration**, do the following:
 - a. For **Connections**, as needed choose **Enable inbound connections** and **Enable outbound connections**.
 - b. For **Allowed protocols**, as needed choose **Enable XA** and **Enable SNA LU**.
8. Under **Scheduling**, choose whether to add the option immediately or at the next maintenance window.
9. Choose **Add option**.

To add this option, no reboot is required.

CLI

To add the MSDTC option

1. Create a JSON file, for example `msdtc-option.json`, with the following required parameters.

```
{  
  "OptionGroupName": "msdtc-se-2016",  
  "OptionsToInclude": [  
    {  
      "OptionName": "MSDTC",  
      "Port": "5000",  
      "VpcSecurityGroupMemberships": ["sg-0abcdef123"],  
      "OptionSettings": [{"Name": "AUTHENTICATION", "Value": "MUTUAL"},  
        {"Name": "TRANSACTION_LOG_SIZE", "Value": "4"}]  
    },  
    "ApplyImmediately": true  
  ]}
```

2. Add the MSDTC option to the option group.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \  
  --cli-input-json file://msdtc-option.json \  
  --apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^  
  --cli-input-json file://msdtc-option.json ^  
  --apply-immediately
```

No reboot is required.

Creating the parameter group for MSDTC

Create or modify a parameter group for the `in-doubt xact resolution` parameter that corresponds to the SQL Server edition and version of your DB instance.

Console

The following example creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose **Create parameter group**.
4. In the **Create parameter group** pane, do the following:
 - a. For **Parameter group family**, choose `sqlserver-se-13.0`.
 - b. For **Group name**, enter an identifier for the parameter group, such as `msdtc-sqlserver-se-13`.
 - c. For **Description**, enter `in-doubt xact resolution`.
5. Choose **Create**.

CLI

The following example creates a parameter group for SQL Server Standard Edition 2016.

To create the parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
--db-parameter-group-name msdtc-sqlserver-se-13 \
--db-parameter-group-family "sqlserver-se-13.0" \
--description "in-doubt xact resolution"
```

For Windows:

```
aws rds create-db-parameter-group ^
--db-parameter-group-name msdtc-sqlserver-se-13 ^
--db-parameter-group-family "sqlserver-se-13.0" ^
--description "in-doubt xact resolution"
```

Modifying the parameter for MSDTC

Modify the `in-doubt xact resolution` parameter in the parameter group that corresponds to the SQL Server edition and version of your DB instance.

For MSDTC, set the `in-doubt xact resolution` parameter to one of the following:

- 1 – `Presume commit`. Any MSDTC in-doubt transactions are presumed to have committed.

- 2 – Presume abort. Any MSDTC in-doubt transactions are presumed to have stopped.

For more information, see [in-doubt xact resolution server configuration option](#) in the Microsoft documentation.

Console

The following example modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Parameter groups**.
3. Choose the parameter group, such as **msdtc-sqlserver-se-13**.
4. Under **Parameters**, filter the parameter list for **xact**.
5. Choose **in-doubt xact resolution**.
6. Choose **Edit parameters**.
7. Enter **1** or **2**.
8. Choose **Save changes**.

CLI

The following example modifies the parameter group that you created for SQL Server Standard Edition 2016.

To modify the parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name msdtc-sqlserver-se-13 \
  --parameters "ParameterName='in-doubt xact
resolution',ParameterValue=1,ApplyMethod=immediate"
```

For Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name msdtc-sqlserver-se-13 ^
  --parameters "ParameterName='in-doubt xact
resolution',ParameterValue=1,ApplyMethod=immediate"
```

Associating the option group and parameter group with the DB instance

You can use the AWS Management Console or the AWS CLI to associate the MSDTC option group and parameter group with the DB instance.

Console

You can associate the MSDTC option group and parameter group with a new or existing DB instance.

- For a new DB instance, associate them when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, associate them by modifying the instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

If you use an domain-joined existing DB instance, it must already have an Active Directory domain and AWS Identity and Access Management (IAM) role associated with it. If you create a new domain-joined instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

CLI

You can associate the MSDTC option group and parameter group with a new or existing DB instance.

Note

If you use an existing domain-joined DB instance, it must already have an Active Directory domain and IAM role associated with it. If you create a new domain-joined instance, specify an existing Active Directory domain and IAM role. For more information, see [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#).

To create a DB instance with the MSDTC option group and parameter group

- Specify the same DB engine type and major version as you used when creating the option group.

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance \
--db-instance-identifier mydbinstance \
--db-instance-class db.m5.2xlarge \
--engine sqlserver-se \
--engine-version 13.00.5426.0.v1 \
--allocated-storage 100 \
--master-user-password secret123 \
--master-username admin \
--storage-type gp2 \
--license-model li \
--domain-iam-role-name my-directory-iam-role \
--domain my-domain-id \
--option-group-name msdtc-se-2016 \
--db-parameter-group-name msdtc-sqlserver-se-13
```

For Windows:

```
aws rds create-db-instance ^
--db-instance-identifier mydbinstance ^
--db-instance-class db.m5.2xlarge ^
--engine sqlserver-se ^
--engine-version 13.00.5426.0.v1 ^
--allocated-storage 100 ^
--master-user-password secret123 ^
--master-username admin ^
--storage-type gp2 ^
--license-model li ^
--domain-iam-role-name my-directory-iam-role ^
--domain my-domain-id ^
--option-group-name msdtc-se-2016 ^
```

```
--db-parameter-group-name msdtc-sqlserver-se-13
```

To modify a DB instance and associate the MSDTC option group and parameter group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--option-group-name msdtc-se-2016 \
--db-parameter-group-name msdtc-sqlserver-se-13 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--option-group-name msdtc-se-2016 ^
--db-parameter-group-name msdtc-sqlserver-se-13 ^
--apply-immediately
```

Using distributed transactions

In Amazon RDS for SQL Server, you run distributed transactions in the same way as distributed transactions running on-premises:

- Using .NET framework System.Transactions promotable transactions, which optimizes distributed transactions by deferring their creation until they're needed.

In this case, promotion is automatic and doesn't require you to make any intervention. If there's only one resource manager within the transaction, no promotion is performed. For more information about implicit transaction scopes, see [Implementing an implicit transaction using transaction scope](#) in the Microsoft documentation.

Promotable transactions are supported with these .NET implementations:

- Starting with ADO.NET 2.0, System.Data.SqlClient supports promotable transactions with SQL Server. For more information, see [System.Transactions integration with SQL Server](#) in the Microsoft documentation.
- ODP.NET supports System.Transactions. A local transaction is created for the first connection opened in the TransactionsScope scope to Oracle Database 11g release 1 (version 11.1) and later. When a second connection is opened, this transaction is automatically promoted to a distributed transaction. For more information about distributed transaction support in ODP.NET, see [Microsoft Distributed Transaction Coordinator integration](#) in the Microsoft documentation.
- Using the BEGIN DISTRIBUTED TRANSACTION statement. For more information, see [BEGIN DISTRIBUTED TRANSACTION \(Transact-SQL\)](#) in the Microsoft documentation.

Using XA transactions

Starting from RDS for SQL Server 2017 version 14.00.3223.3, you can control distributed transactions using JDBC. When you set the Enable_XA option setting to true in the MSDTC option, RDS

automatically enables JDBC transactions and grants the `SqlJDBCXAUser` role to the guest user. This allows executing distributed transactions through JDBC. For more information, including a code example, see [Understanding XA transactions](#) in the Microsoft documentation.

Using transaction tracing

RDS supports controlling MSDTC transaction traces and downloading them from the RDS DB instance for troubleshooting. You can control transaction tracing sessions by running the following RDS stored procedure.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'trace_action',
[@traceall='0|1'],
[@traceaborted='0|1'],
[@tracelong='0|1'];
```

The following parameter is required:

- `trace_action` – The tracing action. It can be START, STOP, or STATUS.

The following parameters are optional:

- `@traceall` – Set to 1 to trace all distributed transactions. The default is 0.
- `@traceaborted` – Set to 1 to trace canceled distributed transactions. The default is 0.
- `@tracelong` – Set to 1 to trace long-running distributed transactions. The default is 0.

Example of START tracing action

To start a new transaction tracing session, run the following example statement.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'START',
@traceall='0',
@traceaborted='1',
@tracelong='1';
```

Note

Only one transaction tracing session can be active at one time. If a new tracing session START command is issued while a tracing session is active, an error is returned and the active tracing session remains unchanged.

Example of STOP tracing action

To stop a transaction tracing session, run the following statement.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STOP'
```

This statement stops the active transaction tracing session and saves the transaction trace data into the log directory on the RDS DB instance. The first row of the output contains the overall result, and the following lines indicate details of the operation.

The following is an example of a successful tracing session stop.

```
OK: Trace session has been successfully stopped.
Setting log file to: D:\rdsdbdata\MSDTC\Trace\dtctrace.log
Examining D:\rdsdbdata\MSDTC\Trace\msdtctr.mof for message formats, 8 found.
```

```
Searching for TMF files on path: (null)
LogFile D:\rdsdbdata\MSDTC\Trace\dtttrace.log:
OS version 10.0.14393 (Currently running on 6.2.9200)
StartTime <timestamp>
EndTime <timestamp>
Timezone is @tzres.dll,-932 (Bias is 0mins)
BufferSize 16384 B
Maximum File Size 10 MB
Buffers Written Not set (Logger may not have been stopped).
Logger Mode Settings (11000002) (circular paged)
ProcessorCount 1
Processing completed Buffers: 1, Events: 3, EventsLost: 0 :: Format Errors: 0, Unknowns: 3
Event traces dumped to d:\rdsdbdata\Log\msdtc_<timestamp>.log
```

You can use the detailed information to query the name of the generated log file. For more information about downloading log files from the RDS DB instance, see [Monitoring Amazon RDS log files \(p. 680\)](#).

The trace session logs remain on the instance for 35 days. Any older trace session logs are automatically deleted.

Example of STATUS tracing action

To trace the status of a transaction tracing session, run the following statement.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STATUS'
```

This statement outputs the following as separate rows of the result set.

```
OK
SessionStatus: <Started|Stopped>
TraceAll: <True|False>
TraceAborted: <True|False>
TraceLongLived: <True|False>
```

The first line indicates the overall result of the operation: OK or ERROR with details, if applicable. The subsequent lines indicate details about the tracing session status:

- SessionStatus can be one of the following:
 - Started if a tracing session is running.
 - Stopped if no tracing session is running.
- The tracing session flags can be True or False depending on how they were set in the START command.

Modifying the MSDTC option

After you enable the MSDTC option, you can modify its settings. For information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#).

Note

Some changes to MSDTC option settings require the MSDTC service to be restarted. This requirement can affect running distributed transactions.

Disabling MSDTC

To disable MSDTC, remove the MSDTC option from its option group.

Console

To remove the MSDTC option from its option group

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Option groups**.
3. Choose the option group with the MSDTC option (msdtc-se-2016 in the previous examples).
4. Choose **Delete option**.
5. Under **Deletion options**, choose **MSDTC for Options to delete**.
6. Under **Apply immediately**, choose **Yes** to delete the option immediately, or **No** to delete it at the next maintenance window.
7. Choose **Delete**.

CLI

To remove the MSDTC option from its option group

- Use one of the following commands.

Example

For Linux, macOS, or Unix:

```
aws rds remove-option-from-option-group \
    --option-group-name msdtc-se-2016 \
    --options MSDTC \
    --apply-immediately
```

For Windows:

```
aws rds remove-option-from-option-group ^
    --option-group-name msdtc-se-2016 ^
    --options MSDTC ^
    --apply-immediately
```

Troubleshooting MSDTC for RDS for SQL Server

In some cases, you might have trouble establishing a connection between MSDTC running on a client computer and the MSDTC service running on an RDS for SQL Server DB instance. If so, make sure of the following:

- The inbound rules for the security group associated with the DB instance are configured correctly. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).
- Your client computer is configured correctly.
- The MSDTC firewall rules on your client computer are enabled.

To configure the client computer

1. Open **Component Services**.

Or, in **Server Manager**, choose **Tools**, and then choose **Component Services**.

2. Expand **Component Services**, expand **Computers**, expand **My Computer**, and then expand **Distributed Transaction Coordinator**.
3. Open the context (right-click) menu for **Local DTC** and choose **Properties**.
4. Choose the **Security** tab.
5. Choose all of the following:
 - **Network DTC Access**
 - **Allow Inbound**
 - **Allow Outbound**
6. Make sure that the correct authentication mode is chosen:
 - **Mutual Authentication Required** – The client machine is joined to the same domain as other nodes participating in distributed transaction, or there is a trust relationship configured between domains.
 - **No Authentication Required** – All other cases.
7. Choose **OK** to save your changes.
8. If prompted to restart the service, choose **Yes**.

To enable MSDTC firewall rules

1. Open Windows Firewall, then choose **Advanced settings**.

Or, in **Server Manager**, choose **Tools**, and then choose **Windows Firewall with Advanced Security**.

Note

Depending on your operating system, Windows Firewall might be called Windows Defender Firewall.

2. Choose **Inbound Rules** in the left pane.
3. Enable the following firewall rules, if they are not already enabled:
 - **Distributed Transaction Coordinator (RPC)**
 - **Distributed Transaction Coordinator (RPC)-EPMAP**
 - **Distributed Transaction Coordinator (TCP-In)**
4. Close Windows Firewall.

Common DBA tasks for Microsoft SQL Server

This section describes the Amazon RDS-specific implementations of some common DBA tasks for DB instances that are running the Microsoft SQL Server database engine. In order to deliver a managed service experience, Amazon RDS does not provide shell access to DB instances, and it restricts access to certain system procedures and tables that require advanced privileges.

Note

When working with a SQL Server DB instance, you can run scripts to modify a newly created database, but you cannot modify the [model] database, the database used as the model for new databases.

Topics

- [Accessing the tempdb database on Microsoft SQL Server DB instances on Amazon RDS \(p. 1292\)](#)
- [Analyzing your database workload on an Amazon RDS for SQL Server DB instance with Database Engine Tuning Advisor \(p. 1294\)](#)
- [Collations and character sets for Microsoft SQL Server \(p. 1296\)](#)
- [Creating a database user \(p. 1299\)](#)
- [Determining a recovery model for your Microsoft SQL Server database \(p. 1300\)](#)
- [Determining the last failover time \(p. 1300\)](#)
- [Disabling fast inserts during bulk loading \(p. 1301\)](#)
- [Dropping a Microsoft SQL Server database \(p. 1301\)](#)
- [Renaming a Microsoft SQL Server database in a Multi-AZ deployment \(p. 1301\)](#)
- [Resetting the db_owner role password \(p. 1302\)](#)
- [Restoring license-terminated DB instances \(p. 1302\)](#)
- [Transitioning a Microsoft SQL Server database from OFFLINE to ONLINE \(p. 1303\)](#)
- [Using change data capture \(p. 1303\)](#)
- [Using SQL Server Agent \(p. 1305\)](#)
- [Working with Microsoft SQL Server logs \(p. 1308\)](#)
- [Working with trace and dump files \(p. 1309\)](#)

Accessing the tempdb database on Microsoft SQL Server DB instances on Amazon RDS

You can access the tempdb database on your Microsoft SQL Server DB instances on Amazon RDS. You can run code on tempdb by using Transact-SQL through Microsoft SQL Server Management Studio (SSMS), or any other standard SQL client application. For more information about connecting to your DB instance, see [Connecting to a DB instance running the Microsoft SQL Server database engine \(p. 1084\)](#).

The master user for your DB instance is granted CONTROL access to tempdb so that this user can modify the tempdb database options. The master user isn't the database owner of the tempdb database. If necessary, the master user can grant CONTROL access to other users so that they can also modify the tempdb database options.

Note

You can't run Database Console Commands (DBCC) on the tempdb database.

Modifying tempdb database options

You can modify the database options on the tempdb database on your Amazon RDS DB instances. For more information about which options can be modified, see [tempdb database](#) in the Microsoft documentation.

Database options such as the maximum file size options are persistent after you restart your DB instance. You can modify the database options to optimize performance when importing data, and to prevent running out of storage.

Optimizing performance when importing data

To optimize performance when importing large amounts of data into your DB instance, set the SIZE and FILEGROWTH properties of the tempdb database to large numbers. For more information about how to optimize tempdb, see [Optimizing tempdb performance](#) in the Microsoft documentation.

The following example demonstrates setting the size to 100 GB and file growth to 10 percent.

```
alter database[tempdb] modify file (NAME = N'templog', SIZE=100GB, FILEGROWTH = 10%)
```

Preventing storage problems

To prevent the tempdb database from using all available disk space, set the MAXSIZE property. The following example demonstrates setting the property to 2048 MB.

```
alter database [tempdb] modify file (NAME = N'templog', MAXSIZE = 2048MB)
```

Shrinking the tempdb database

There are two ways to shrink the tempdb database on your Amazon RDS DB instance. You can use the `rds_shrink_tempdbfile` procedure, or you can set the SIZE property,

Using the `rds_shrink_tempdbfile` procedure

You can use the Amazon RDS procedure `msdb.dbo.rds_shrink_tempdbfile` to shrink the tempdb database. You can only call `rds_shrink_tempdbfile` if you have CONTROL access to tempdb. When you call `rds_shrink_tempdbfile`, there is no downtime for your DB instance.

The `rds_shrink_tempdbfile` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>@temp_filename</code>	SYSNAME	—	required	The logical name of the file to shrink.
<code>@target_size</code>	int	null	optional	The new size for the file, in megabytes.

The following example gets the names of the files for the tempdb database.

```
use tempdb;
GO

select name, * from sys.sysfiles;
GO
```

The following example shrinks a tempdb database file named `test_file`, and requests a new size of 10 megabytes:

```
exec msdb.dbo.rds_shrink_tempdbfile @temp_filename = N'test_file', @target_size = 10;
```

Setting the SIZE property

You can also shrink the tempdb database by setting the SIZE property and then restarting your DB instance. For more information about restarting your DB instance, see [Rebooting a DB instance \(p. 366\)](#).

The following example demonstrates setting the SIZE property to 1024 MB.

```
alter database [tempdb] modify file (NAME = N'templog', SIZE = 1024MB)
```

Considerations for Multi-AZ deployments

If your Amazon RDS DB instance is in a Multi-AZ Deployment for Microsoft SQL Server with Database Mirroring (DBM) or Always On Availability Groups (AGs), there are some things to consider.

The tempdb database can't be replicated. No data that you store on your primary instance is replicated to your secondary instance.

If you modify any database options on the tempdb database, you can capture those changes on the secondary by using one of the following methods:

- First modify your DB instance and turn Multi-AZ off, then modify tempdb, and finally turn Multi-AZ back on. This method doesn't involve any downtime.

For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- First modify tempdb in the original primary instance, then fail over manually, and finally modify tempdb in the new primary instance. This method involves downtime.

For more information, see [Rebooting a DB instance \(p. 366\)](#).

Analyzing your database workload on an Amazon RDS for SQL Server DB instance with Database Engine Tuning Advisor

Database Engine Tuning Advisor is a client application provided by Microsoft that analyzes database workload and recommends an optimal set of indexes for your Microsoft SQL Server databases based on the kinds of queries you run. Like SQL Server Management Studio, you run Tuning Advisor from a client computer that connects to your Amazon RDS DB instance that is running SQL Server. The client computer can be a local computer that you run on premises within your own network or it can be an Amazon EC2 Windows instance that is running in the same region as your Amazon RDS DB instance.

This section shows how to capture a workload for Tuning Advisor to analyze. This is the preferred process for capturing a workload because Amazon RDS restricts host access to the SQL Server instance. For more information, see [Database Engine Tuning Advisor](#) in the Microsoft documentation.

To use Tuning Advisor, you must provide what is called a workload to the advisor. A workload is a set of Transact-SQL statements that run against a database or databases that you want to tune. Database Engine Tuning Advisor uses trace files, trace tables, Transact-SQL scripts, or XML files as workload input when tuning databases. When working with Amazon RDS, a workload can be a file on a client computer or a database table on an Amazon RDS for SQL Server DB accessible to your client computer. The file or the table must contain queries against the databases you want to tune in a format suitable for replay.

For Tuning Advisor to be most effective, a workload should be as realistic as possible. You can generate a workload file or table by performing a trace against your DB instance. While a trace is running, you can either simulate a load on your DB instance or run your applications with a normal load.

There are two types of traces: client-side and server-side. A client-side trace is easier to set up and you can watch trace events being captured in real-time in SQL Server Profiler. A server-side trace is more complex to set up and requires some Transact-SQL scripting. In addition, because the trace is written to a file on the Amazon RDS DB instance, storage space is consumed by the trace. It is important to track of how much storage space a running server-side trace uses because the DB instance could enter a storage-full state and would no longer be available if it runs out of storage space.

For a client-side trace, when a sufficient amount of trace data has been captured in the SQL Server Profiler, you can then generate the workload file by saving the trace to either a file on your local computer or in a database table on a DB instance that is available to your client computer. The main disadvantage of using a client-side trace is that the trace may not capture all queries when under heavy loads. This could weaken the effectiveness of the analysis performed by the Database Engine Tuning Advisor. If you need to run a trace under heavy loads and you want to ensure that it captures every query during a trace session, you should use a server-side trace.

For a server-side trace, you must get the trace files on the DB instance into a suitable workload file or you can save the trace to a table on the DB instance after the trace completes. You can use the SQL Server Profiler to save the trace to a file on your local computer or have the Tuning Advisor read from the trace table on the DB instance.

Running a client-side trace on a SQL Server DB instance

To run a client-side trace on a SQL Server DB instance

1. Start SQL Server Profiler. It is installed in the Performance Tools folder of your SQL Server instance folder. You must load or define a trace definition template to start a client-side trace.
2. In the SQL Server Profiler File menu, choose **New Trace**. In the **Connect to Server** dialog box, enter the DB instance endpoint, port, master user name, and password of the database you would like to run a trace on.

3. In the **Trace Properties** dialog box, enter a trace name and choose a trace definition template. A default template, TSQL_Replay, ships with the application. You can edit this template to define your trace. Edit events and event information under the **Events Selection** tab of the **Trace Properties** dialog box.

For more information about trace definition templates and using the SQL Server Profiler to specify a client-side trace, see [Database Engine Tuning Advisor](#) in the Microsoft documentation.
4. Start the client-side trace and watch SQL queries in real-time as they run against your DB instance.
5. Select **Stop Trace** from the **File** menu when you have completed the trace. Save the results as a file or as a trace table on your DB instance.

Running a server-side trace on a SQL Server DB instance

Writing scripts to create a server-side trace can be complex and is beyond the scope of this document. This section contains sample scripts that you can use as examples. As with a client-side trace, the goal is to create a workload file or trace table that you can open using the Database Engine Tuning Advisor.

The following is an abridged example script that starts a server-side trace and captures details to a workload file. The trace initially saves to the file RDSTrace.trc in the D:\RDSDBDATA\Log directory and rolls-over every 100 MB so subsequent trace files are named RDSTrace_1.trc, RDSTrace_2.trc, etc.

```
DECLARE @file_name NVARCHAR(245) = 'D:\RDSDBDATA\Log\RDSTrace';
DECLARE @max_file_size BIGINT = 100;
DECLARE @on BIT = 1
DECLARE @rc INT
DECLARE @traceid INT

EXEC @rc = sp_trace_create @traceid OUTPUT, 2, @file_name, @max_file_size
IF (@rc = 0) BEGIN
    EXEC sp_trace_setevent @traceid, 10, 1, @on
    EXEC sp_trace_setevent @traceid, 10, 2, @on
    EXEC sp_trace_setevent @traceid, 10, 3, @on
    .
    .
    EXEC sp_trace_setfilter @traceid, 10, 0, 7, N'SQL Profiler'
    EXEC sp_trace_setstatus @traceid, 1
END
```

The following example is a script that stops a trace. Note that a trace created by the previous script continues to run until you explicitly stop the trace or the process runs out of disk space.

```
DECLARE @traceid INT
SELECT @traceid = traceid FROM ::fn_trace_getinfo(default)
WHERE property = 5 AND value = 1 AND traceid <> 1

IF @traceid IS NOT NULL BEGIN
    EXEC sp_trace_setstatus @traceid, 0
    EXEC sp_trace_setstatus @traceid, 2
END
```

You can save server-side trace results to a database table and use the database table as the workload for the Tuning Advisor by using the fn_trace_gettable function. The following commands load the results of all files named RDSTrace.trc in the D:\rdsdbdata\Log directory, including all rollover files like RDSTrace_1.trc, into a table named RDSTrace in the current database.

```
SELECT * INTO RDSTrace
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace.trc', default);
```

To save a specific rollover file to a table, for example the RDSTrace_1.trc file, specify the name of the rollover file and substitute 1 instead of default as the last parameter to fn_trace_gettable.

```
SELECT * INTO RDSTrace_1
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace_1.trc', 1);
```

Running Tuning Advisor with a trace

Once you create a trace, either as a local file or as a database table, you can then run Tuning Advisor against your DB instance. Using Tuning Advisor with Amazon RDS is the same process as when working with a standalone, remote SQL Server instance. You can either use the Tuning Advisor UI on your client machine or use the dta.exe utility from the command line. In both cases, you must connect to the Amazon RDS DB instance using the endpoint for the DB instance and provide your master user name and master user password when using Tuning Advisor.

The following code example demonstrates using the dta.exe command line utility against an Amazon RDS DB instance with an endpoint of **dta.cnazcmklsdei.us-east-1.rds.amazonaws.com**. The example includes the master user name **admin** and the master user password **test**, the example database to tune is named machine named **C:\RDSTrace.trc**. The example command line code also specifies a trace session named **RDSTrace1** and specifies output files to the local machine named **RDSTrace.sql** for the SQL output script, **RDSTrace.txt** for a result file, and **RDSTrace.xml** for an XML file of the analysis. There is also an error table specified on the RDSDTA database named **RDSTraceErrors**.

```
dta -S dta.cnazcmklsdei.us-east-1.rds.amazonaws.com -U admin -P test -D RDSDTA -if C:\RDSTrace.trc -s RDSTrace1 -of C:\RDSTrace.sql -or C:\RDSTrace.txt -ox C:\RDSTrace.xml -e RDSDTA.dbo.RDSTraceErrors
```

Here is the same example command line code except the input workload is a table on the remote Amazon RDS instance named **RDSTrace** which is on the **RDSDTA** database.

```
dta -S dta.cnazcmklsdei.us-east-1.rds.amazonaws.com -U admin -P test -D RDSDTA -it RDSDTA.dbo.RDSTrace -s RDSTrace1 -of C:\RDSTrace.sql -or C:\RDSTrace.txt -ox C:\RDSTrace.xml -e RDSDTA.dbo.RDSTraceErrors
```

For a full list of dta utility command-line parameters, see [dta Utility](#) in the Microsoft documentation.

Collations and character sets for Microsoft SQL Server

SQL Server supports collations at multiple levels. You set the default server collation when you create the DB instance. You can override the collation in the database, table, or column level.

Topics

- [Server-level collation for Microsoft SQL Server \(p. 1296\)](#)
- [Database-level collation for Microsoft SQL Server \(p. 1299\)](#)

Server-level collation for Microsoft SQL Server

When you create a Microsoft SQL Server DB instance, you can set the server collation that you want to use. If you don't choose a different collation, the server-level collation defaults to **SQL_Latin1_General_CI_AS**. The server collation is applied by default to all databases and database objects.

Note

You can't change the collation when you restore from a DB snapshot.

Currently, Amazon RDS supports the following server collations:

Collation	Description
Chinese_PRC_BIN2	Chinese-PRC, binary code point sort order
Chinese_PRC_CI_AS	Chinese-PRC, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Chinese_Taiwan_Stroke_CI_AS	Chinese-Taiwan-Stroke, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Danish_Norwegian_CI_AS	Danish-Norwegian, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Finnish_Swedish_CI_AS	Finnish, Swedish, and Swedish (Finland), case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
French_CI_AS	French, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Hebrew_BIN	Hebrew, binary sort
Hebrew_CI_AS	Hebrew, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Japanese_BIN	Japanese, binary sort
Japanese_CI_AS	Japanese, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Japanese_CS_AS	Japanese, case-sensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Korean_Wansung_CI_AS	Korean-Wansung, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Latin1_General_100_BIN	Latin1-General-100, binary sort
Latin1_General_100_BIN2	Latin1-General-100, binary code point sort order
Latin1_General_100_CI_AS	Latin1-General-100, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Latin1_General_BIN	Latin1-General, binary sort
Latin1_General_BIN2	Latin1-General, binary code point sort order
Latin1_General_CI_AI	Latin1-General, case-insensitive, accent-insensitive, kanatype-insensitive, width-insensitive
Latin1_General_CI_AS	Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Latin1_General_CI_AS_KS	Latin1-General, case-insensitive, accent-sensitive, kanatype-sensitive, width-insensitive

Collation	Description
Latin1_General_CS_AS	Latin1-General, case-sensitive, accent-sensitive, kanatype-insensitive, width-insensitive
Modern_Spanish_CI_AS	Modern-Spanish, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive
SQL_1xCompat_CP850_CI_AS	Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 49 on Code Page 850 for non-Unicode Data
SQL_Latin1_General_CP1_CI_AI	Latin1-General, case-insensitive, accent-insensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 54 on Code Page 1252 for non-Unicode Data
SQL_Latin1_General_CP1_CI_AS (default)	Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data
SQL_Latin1_General_CP1_CS_AS	Latin1-General, case-sensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 51 on Code Page 1252 for non-Unicode Data
SQL_Latin1_General_CP437_CI_AI	Latin1-General, case-insensitive, accent-insensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 34 on Code Page 437 for non-Unicode Data
SQL_Latin1_General_CP850_BIN2	Latin1-General, binary code point sort order for Unicode Data, SQL Server Sort Order 40 on Code Page 850 for non-Unicode Data
SQL_Latin1_General_CP850_CI_AS	Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 42 on Code Page 850 for non-Unicode Data
SQL_Latin1_General_CP1256_CI_AS	Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 146 on Code Page 1256 for non-Unicode Data
Thai_CI_AS	Thai, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive

To choose the collation:

- If you're using the Amazon RDS console, when creating a new DB instance choose **Additional configuration**, then choose the collation from the **Collation** menu under **Database options**. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- If you're using the AWS CLI, use the `--character-set-name` option with the `create-db-instance` command. For more information, see [create-db-instance](#).

- If you're using the Amazon RDS API, use the `CharacterSetName` parameter with the `CreateDBInstance` operation. For more information, see [CreateDBInstance](#).

Database-level collation for Microsoft SQL Server

You can change the default collation at the database, table, or column level by overriding the collation when creating a new database or database object. For example, if your default server collation is `SQL_Latin1_General_CI_AS`, you can change it to `Mohawk_100_CI_AS` for Mohawk collation support. Even arguments in a query can be type-cast to use a different collation if necessary.

For example, the following query would change the default collation for the `AccountName` column to `Mohawk_100_CI_AS`

```
CREATE TABLE [dbo].[Account]
(
    [AccountID] [nvarchar](10) NOT NULL,
    [AccountName] [nvarchar](100) COLLATE Mohawk_100_CI_AS NOT NULL
) ON [PRIMARY];
```

The Microsoft SQL Server DB engine supports Unicode by the built-in `NCHAR`, `NVARCHAR`, and `NTEXT` data types. For example, if you need CJK support, use these Unicode data types for character storage and override the default server collation when creating your databases and tables. Here are several links from Microsoft covering collation and Unicode support for SQL Server:

- [Working with collations](#)
- [Collation and international terminology](#)
- [Using SQL Server collations](#)
- [International considerations for databases and database engine applications](#)

Creating a database user

You can create a database user for your Amazon RDS for Microsoft SQL Server DB instance by running a T-SQL script like the following example. Use an application such as SQL Server Management Suite (SSMS). You log into the DB instance as the master user that was created when you created the DB instance.

```
--Initially set context to master database
USE [master];
GO
--Create a server-level login named theirname with password theirpassword
CREATE LOGIN [theirname] WITH PASSWORD = 'theirpassword';
GO
--Set context to msdb database
USE [msdb];
GO
--Create a database user named theirname and link it to server-level login theirname
CREATE USER [theirname] FOR LOGIN [theirname];
GO
```

For an example of adding a database user to a role, see [Adding a user to the SQLAgentUser role \(p. 1307\)](#).

Note

If you get permission errors when adding a user, you can restore privileges by modifying the DB instance master user password. For more information, see [Resetting the db_owner role password \(p. 1302\)](#).

Determining a recovery model for your Microsoft SQL Server database

In Amazon RDS, the recovery model, retention period, and database status are linked.

It's important to understand the consequences before making a change to one of these settings. Each setting can affect the others. For example:

- If you change a database's recovery model to SIMPLE or BULK_LOGGED while backup retention is enabled, Amazon RDS resets the recovery model to FULL within five minutes. This also results in RDS taking a snapshot of the DB instance.
- If you set backup retention to 0 days, RDS sets the recovery mode to SIMPLE.
- If you change a database's recovery model from SIMPLE to any other option while backup retention is set to 0 days, RDS resets the recovery model to SIMPLE.

Important

Never change the recovery model on Multi-AZ instances, even if it seems you can do so—for example, by using ALTER DATABASE. Backup retention, and therefore FULL recovery mode, is required for Multi-AZ. If you alter the recovery model, RDS immediately changes it back to FULL. This automatic reset forces RDS to completely rebuild the mirror. During this rebuild, the availability of the database is degraded for about 30-90 minutes until the mirror is ready for failover. The DB instance also experiences performance degradation in the same way it does during a conversion from Single-AZ to Multi-AZ. How long performance is degraded depends on the database storage size—the bigger the stored database, the longer the degradation.

For more information on SQL Server recovery models, see [Recovery models \(SQL Server\)](#) in the Microsoft documentation.

Determining the last failover time

To determine the last failover time, use the following stored procedure:

```
execute msdb.dbo.rds_failover_time;
```

This procedure returns the following information.

Output parameter	Description
errorlog_available_from	Shows the time from when error logs are available in the log directory.
recent_failover_time	Shows the last failover time if it's available from the error logs. Otherwise it shows null.

Note

The stored procedure searches all of the available SQL Server error logs in the log directory to retrieve the most recent failover time. If the failover messages have been overwritten by SQL Server, then the procedure doesn't retrieve the failover time.

Example of no recent failover

This example shows the output when there is no recent failover in the error logs. No failover has happened since 2020-04-29 23:59:00.01.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example of recent failover

This example shows the output when there is a failover in the error logs. The most recent failover was at 2020-05-05 18:57:51.89.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Disabling fast inserts during bulk loading

Starting with SQL Server 2016, fast inserts are enabled by default. Fast inserts leverage the minimal logging that occurs while the database is in the simple or bulk logged recovery model to optimize insert performance. With fast inserts, each bulk load batch acquires new extents, bypassing the allocation lookup for existing extents with available free space to optimize insert performance.

However, with fast inserts bulk loads with small batch sizes can lead to increased unused space consumed by objects. If increasing batch size isn't feasible, enabling trace flag 692 can help reduce unused reserved space, but at the expense of performance. Enabling this trace flag disables fast inserts while bulk loading data into heap or clustered indexes.

You enable trace flag 692 as a startup parameter using DB parameter groups. For more information, see [Working with parameter groups \(p. 289\)](#).

Trace flag 692 is supported for Amazon RDS on SQL Server 2016 and later. For more information on trace flags, see [DBCC TRACEON - trace flags](#) in the Microsoft documentation.

Dropping a Microsoft SQL Server database

You can drop a database on an Amazon RDS DB instance running Microsoft SQL Server in a Single-AZ or Multi-AZ deployment. To drop the database, use the following command:

```
--replace your-database-name with the name of the database you want to drop  
EXECUTE msdb.dbo.rds_drop_database N'your-database-name'
```

Note

Use straight single quotes in the command. Smart quotes will cause an error.

After you use this procedure to drop the database, Amazon RDS drops all existing connections to the database and removes the database's backup history.

Renaming a Microsoft SQL Server database in a Multi-AZ deployment

To rename a Microsoft SQL Server database instance that uses Multi-AZ, use the following procedure:

1. First, turn off Multi-AZ for the DB instance.
2. Rename the database by running `rdsadmin.dbo.rds_modify_db_name`.

3. Then, turn on Multi-AZ Mirroring or Always On Availability Groups for the DB instance, to return it to its original state.

For more information, see [Adding Multi-AZ to a Microsoft SQL Server DB instance \(p. 1130\)](#).

Note

If your instance doesn't use Multi-AZ, you don't need to change any settings before or after running `rdsadmin.dbo.rds_modify_db_name`.

Example: In the following example, the `rdsadmin.dbo.rds_modify_db_name` stored procedure renames a database from **M00** to **ZAR**. This is similar to running the statement `DDL ALTER DATABASE [M00] MODIFY NAME = [ZAR]`.

```
EXEC rdsadmin.dbo.rds_modify_db_name N'M00', N'ZAR'  
GO
```

Resetting the db_owner role password

If you lock yourself out of the db_owner role on your Microsoft SQL Server database, you can reset the db_owner role password by modifying the DB instance master password. By changing the DB instance master password, you can regain access to the DB instance, access databases using the modified password for the db_owner, and restore privileges for the db_owner role that may have been accidentally revoked. You can change the DB instance password by using the Amazon RDS console, the AWS CLI command [modify-db-instance](#), or by using the [ModifyDBInstance](#) operation. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Restoring license-terminated DB instances

Microsoft has requested that some Amazon RDS customers who did not report their Microsoft License Mobility information terminate their DB instance. Amazon RDS takes snapshots of these DB instances, and you can restore from the snapshot to a new DB instance that has the License Included model.

You can restore from a snapshot of Standard Edition to either Standard Edition or Enterprise Edition.

You can restore from a snapshot of Enterprise Edition to either Standard Edition or Enterprise Edition.

To restore from a SQL Server snapshot after Amazon RDS has created a final snapshot of your instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the snapshot of your SQL Server DB instance. Amazon RDS creates a final snapshot of your DB instance. The name of the terminated instance snapshot is in the format `instance_name-final-snapshot`. For example, if your DB instance name is `mytest.cdxgahs1ksma.us-east-1.rds.com`, the final snapshot is called `mytest-final-snapshot` and is located in the same AWS Region as the original DB instance.
4. For **Actions**, choose **Restore Snapshot**.

The **Restore DB Instance** window appears.

5. For **License Model**, choose **license-included**.
6. Choose the SQL Server DB engine that you want to use.
7. For **DB Instance Identifier**, enter the name for the restored DB instance.

8. Choose **Restore DB Instance**.

For more information about restoring from a snapshot, see [Restoring from a DB snapshot \(p. 452\)](#).

Transitioning a Microsoft SQL Server database from OFFLINE to ONLINE

You can transition your Microsoft SQL Server database on an Amazon RDS DB instance from OFFLINE to ONLINE.

SQL Server method	Amazon RDS method
ALTER DATABASE <i>db_name</i> SET ONLINE;	EXEC rdsadmin.dbo.rds_set_database_online <i>db_name</i>

Using change data capture

Amazon RDS supports change data capture (CDC) for your DB instances running Microsoft SQL Server. CDC captures changes that are made to the data in your tables. It stores metadata about each change, which you can access later. For more information about how CDC works, see [Change data capture](#) in the Microsoft documentation.

Before you use CDC with your Amazon RDS DB instances, enable it in the database by running `msdb.dbo.rds_cdc_enable_db`. You must have master user privileges to enable CDC in the Amazon RDS DB instance. After CDC is enabled, any user who is `db_owner` of that database can enable or disable CDC on tables in that database.

Important

During restores, CDC will be disabled. All of the related metadata is automatically removed from the database. This applies to snapshot restores, point-in-time restores, and SQL Server Native restores from S3. After performing one of these types of restores, you can re-enable CDC and re-specify tables to track.

To enable CDC for a DB instance, run the `msdb.dbo.rds_cdc_enable_db` stored procedure.

```
exec msdb.dbo.rds_cdc_enable_db 'database_name'
```

To disable CDC for a DB instance, run the `msdb.dbo.rds_cdc_disable_db` stored procedure.

```
exec msdb.dbo.rds_cdc_disable_db 'database_name'
```

Topics

- [Tracking tables with change data capture \(p. 1303\)](#)
- [Change data capture jobs \(p. 1304\)](#)
- [Change data capture for Multi-AZ instances \(p. 1304\)](#)

Tracking tables with change data capture

After CDC is enabled on the database, you can start tracking specific tables. You can choose the tables to track by running [`sys.sp_cdc_enable_table`](#).

```
--Begin tracking a table
exec sys.sp_cdc_enable_table
    @source_schema      = N'source_schema'
    , @source_name       = N'source_name'
    , @role_name         = N'role_name'

--The following parameters are optional:
--, @capture_instance      = 'capture_instance'
--, @supports_net_changes  = supports_net_changes
--, @index_name             = 'index_name'
--, @captured_column_list   = 'captured_column_list'
--, @filegroup_name         = 'filegroup_name'
--, @allow_partition_switch = 'allow_partition_switch'
;
```

To view the CDC configuration for your tables, run [sys.sp_cdc_help_change_data_capture](#).

```
--View CDC configuration
exec sys.sp_cdc_help_change_data_capture

--The following parameters are optional and must be used together.
--  'schema_name', 'table_name'
;
```

For more information on CDC tables, functions, and stored procedures in SQL Server documentation, see the following:

- [Change data capture stored procedures \(Transact-SQL\)](#)
- [Change data capture functions \(Transact-SQL\)](#)
- [Change data capture tables \(Transact-SQL\)](#)

Change data capture jobs

When you enable CDC, SQL Server creates the CDC jobs. Database owners (`db_owner`) can view, create, modify, and delete the CDC jobs. However, the RDS system account owns them. Therefore, the jobs aren't visible from native views, procedures, or in SQL Server Management Studio.

To control behavior of CDC in a database, use native SQL Server procedures such as `sp_cdc_enable_table` and `sp_cdc_start_job`. To change CDC job parameters, like `maxtrans` and `maxscans`, you can use `sp_cdc_change_job..`

To get more information regarding the CDC jobs, you can query the following dynamic management views:

- `sys.dm_cdc_errors`
- `sys.dm_cdc_log_scan_sessions`
- `sysjobs`
- `sysjobhistory`

Change data capture for Multi-AZ instances

If you use CDC on a Multi-AZ instance, make sure the mirror's CDC job configuration matches the one on the principal. CDC jobs are mapped to the `database_id`. If the database IDs on the secondary

are different from the principal, then the jobs won't be associated with the correct database. To try to prevent errors after failover, RDS drops and recreates the jobs on the new principal. The recreated jobs use the parameters that the principal recorded before failover.

Although this process runs quickly, it's still possible that the CDC jobs might run before RDS can correct them. Here are three ways to force parameters to be consistent between primary and secondary replicas:

- Use the same job parameters for all the databases that have CDC enabled.
- Before you change the CDC job configuration, convert the Multi-AZ instance to Single-AZ.
- Manually transfer the parameters whenever you change them on the principal.

To view and define the CDC parameters that are used to recreate the CDC jobs after a failover, use `rds_show_configuration` and `rds_set_configuration`.

The following example returns the value set for `cdc_capture_maxtrans`. For any parameter that is set to `RDS_DEFAULT`, RDS automatically configures the value.

```
-- Show configuration for each parameter on either primary and secondary replicas.  
exec rdsadmin.dbo.rds_show_configuration 'cdc_capture_maxtrans';
```

To set the configuration on the secondary, run `rdsadmin.dbo.rds_set_configuration`. This procedure sets the parameter values for all of the databases on the secondary server. These settings are used only after a failover. The following example sets the `maxtrans` for all CDC capture jobs to `1000`:

```
--To set values on secondary. These are used after failover.  
exec rdsadmin.dbo.rds_set_configuration 'cdc_capture_maxtrans', 1000;
```

To set the CDC job parameters on the principal, use `sys.sp_cdc_change_job` instead.

Using SQL Server Agent

With Amazon RDS, you can use SQL Server Agent on a DB instance running Microsoft SQL Server Enterprise Edition, Standard Edition, or Web Edition. SQL Server Agent is a Microsoft Windows service that runs scheduled administrative tasks that are called jobs. You can use SQL Server Agent to run T-SQL jobs to rebuild indexes, run corruption checks, and aggregate data in a SQL Server DB instance.

When you create a SQL Server DB instance, the master user is enrolled in the `SQLAgentUserRole` role.

SQL Server Agent can run a job on a schedule, in response to a specific event, or on demand. For more information, see [SQL Server Agent](#) in the Microsoft documentation.

Note

Avoid scheduling jobs to run during the maintenance and backup windows for your DB instance. The maintenance and backup processes that are launched by AWS could interrupt a job or cause it to be canceled.

In Multi-AZ deployments, SQL Server Agent jobs are replicated from the primary host to the secondary host when the job replication feature is turned on. For more information, see [Turning on SQL Server Agent job replication \(p. 1306\)](#).

Multi-AZ deployments have a limit of 100 SQL Server Agent jobs. If you need a higher limit, request an increase by contacting AWS Support. Open the [AWS Support Center](#) page, sign in if necessary, and choose **Create case**. Choose **Service limit increase**. Complete and submit the form.

To view the history of an individual SQL Server Agent job in SQL Server Management Studio (SSMS), open Object Explorer, right-click the job, and then choose **View History**.

Because SQL Server Agent is running on a managed host in a DB instance, some actions aren't supported:

- Running replication jobs and running command-line scripts by using ActiveX, Windows command shell, or Windows PowerShell aren't supported.
- You can't manually start, stop, or restart SQL Server Agent.
- Email notifications through SQL Server Agent aren't available from a DB instance.
- SQL Server Agent alerts and operators aren't supported.
- Using SQL Server Agent to create backups isn't supported. Use Amazon RDS to back up your DB instance.

Turning on SQL Server Agent job replication

You can turn on SQL Server Agent job replication by using the following stored procedure:

```
EXECUTE msdb.dbo.rds_set_system_database_sync_objects @object_types = 'SQLAgentJob';
```

You can run the stored procedure on all SQL Server versions supported by Amazon RDS for SQL Server. Jobs in the following categories are replicated:

- [Uncategorized (Local)]
- [Uncategorized (Multi-Server)]
- [Uncategorized]
- Data Collector
- Database Engine Tuning Advisor
- Database Maintenance
- Full-Text

Only jobs that use T-SQL job steps are replicated. Jobs with step types such as SQL Server Integration Services (SSIS), SQL Server Reporting Services (SSRS), Replication, and PowerShell aren't replicated. Jobs that use Database Mail and server-level objects aren't replicated.

Important

The primary host is the source of truth for replication. Before turning on job replication, make sure that your SQL Server Agent jobs are on the primary. If you don't do this, it could lead to the deletion of your SQL Server Agent jobs if you turn on the feature when newer jobs are on the secondary host.

You can use the following function to confirm whether replication is turned on.

```
SELECT * from msdb.dbo.rds_fn_get_system_database_sync_objects();
```

The T-SQL query returns the following if SQL Server Agent jobs are replicating. If they're not replicating, it returns nothing for object_class.

object_class
SQLAgentJob

You can use the following function to find the last time objects were synchronized.

```
SELECT * from msdb.dbo.rds_fn_server_object_last_sync_time();
```

For example, suppose that you modify a SQL Server Agent job at 01:00. You expect the most recent synchronization time to be after 01:00, indicating that synchronization has taken place.

SELECT * from msdb.dbo.rds_fn_server_object_last_sync_time();	
100 %	
Results	Messages
object_class	last_sync_time
1	SQLAgentJob 2022-03-29 01:21:23.6300000

Adding a user to the SQLAgentUserRole role

To allow an additional login or user to use SQL Server Agent, log in as the master user and do the following:

1. Create another server-level login by using the CREATE LOGIN command.
2. Create a user in msdb using CREATE USER command, and then link this user to the login that you created in the previous step.
3. Add the user to the SQLAgentUserRole using the sp_addrolemember system stored procedure.

For example, suppose that your master user name is **admin** and you want to give access to SQL Server Agent to a user named **theirname** with a password **theirpassword**. In that case, you can use the following procedure.

To add a user to the SQLAgentUserRole role

1. Log in as the master user.
2. Run the following commands:

```
--Initially set context to master database
USE [master];
GO
--Create a server-level login named theirname with password theirpassword
CREATE LOGIN [theirname] WITH PASSWORD = 'theirpassword';
GO
--Set context to msdb database
USE [msdb];
GO
--Create a database user named theirname and link it to server-level login theirname
CREATE USER [theirname] FOR LOGIN [theirname];
GO
--Added database user theirname in msdb to SQLAgentUserRole in msdb
EXEC sp_addrolemember [SQLAgentUserRole], [theirname];
```

Deleting a SQL Server Agent job

You use the sp_delete_job stored procedure to delete SQL Server Agent jobs on Amazon RDS for Microsoft SQL Server.

You can't use SSMS to delete SQL Server Agent jobs. If you try to do so, you get an error message similar to the following:

```
The EXECUTE permission was denied on the object 'xp_regrep', database
'mssqlsystemresource', schema 'sys'.
```

As a managed service, RDS is restricted from running procedures that access the Windows registry. When you use SSMS, it tries to run a process (xp_regrep) for which RDS isn't authorized.

Note

On RDS for SQL Server, only members of the sysadmin role are allowed to update or delete jobs owned by a different login.

To delete a SQL Server Agent job

- Run the following T-SQL statement:

```
EXEC msdb..sp_delete_job @job_name = 'job_name';
```

Working with Microsoft SQL Server logs

You can use the Amazon RDS console to view, watch, and download SQL Server Agent logs, Microsoft SQL Server error logs, and SQL Server Reporting Services (SSRS) logs.

Watching log files

If you view a log in the Amazon RDS console, you can see its contents as they exist at that moment. Watching a log in the console opens it in a dynamic state so that you can see updates to it in near-real time.

Only the latest log is active for watching. For example, suppose you have the following logs shown:

Name	Last Written	Size	view	watch	download
log/ERROR	January 14, 2015 at 5:17:35 AM UTC-8	6.1 kB	view	watch	download
log/ERROR.1	January 13, 2015 at 3:59:00 PM UTC-8	53.3 kB	view	watch	download
log/ERROR.2	January 12, 2015 at 3:59:00 PM UTC-8	5.9 kB	view	watch	download
log/ERROR.3	January 11, 2015 at 3:59:00 PM UTC-8	5.9 kB	view	watch	download
log/ERROR.4	January 10, 2015 at 3:59:00 PM UTC-8	5.9 kB	view	watch	download

Only log/ERROR, as the most recent log, is being actively updated. You can choose to watch others, but they are static and will not update.

Archiving log files

The Amazon RDS console shows logs for the past week through the current day. You can download and archive logs to keep them for reference past that time. One way to archive logs is to load them into an Amazon S3 bucket. For instructions on how to set up an Amazon S3 bucket and upload a file, see [Amazon S3 basics](#) in the *Amazon Simple Storage Service Getting Started Guide* and click **Get Started**.

Viewing error and agent logs

To view Microsoft SQL Server error and agent logs, use the Amazon RDS stored procedure `rds_read_error_log` with the following parameters:

- eindex** – the version of the log to retrieve. The default value is 0, which retrieves the current error log. Specify 1 to retrieve the previous log, specify 2 to retrieve the one before that, and so on.
- etype** – the type of log to retrieve. Specify 1 to retrieve an error log. Specify 2 to retrieve an agent log.

Example

The following example requests the current error log.

```
EXEC rdsadmin.dbo.rds_read_error_log @index = 0, @type = 1;
```

For more information on SQL Server errors, see [Database engine errors](#) in the Microsoft documentation.

Working with trace and dump files

This section describes working with trace files and dump files for your Amazon RDS DB instances running Microsoft SQL Server.

Generating a trace SQL query

```
declare @rc int
declare @TraceID int
declare @maxfilesize bigint
set @maxfilesize = 5
exec @rc = sp_trace_create @TraceID output, 0, N'D:\rdsdbdata\log\rdstest', @maxfilesize,
NULL
```

Viewing an open trace

```
select * from ::fn_trace_getinfo(default)
```

Viewing trace contents

```
select * from ::fn_trace_gettable('D:\rdsdbdata\log\rdstest.trc', default)
```

Setting the retention period for trace and dump files

Trace and dump files can accumulate and consume disk space. By default, Amazon RDS purges trace and dump files that are older than seven days.

To view the current trace and dump file retention period, use the `rds_show_configuration` procedure, as shown in the following example.

```
exec rdsadmin..rds_show_configuration;
```

To modify the retention period for trace files, use the `rds_set_configuration` procedure and set the `tracefile retention` in minutes. The following example sets the trace file retention period to 24 hours.

```
exec rdsadmin..rds_set_configuration 'tracefile retention', 1440;
```

To modify the retention period for dump files, use the `rds_set_configuration` procedure and set the `dumpfile retention` in minutes. The following example sets the dump file retention period to 3 days.

```
exec rdsadmin..rds_set_configuration 'dumpfile retention', 4320;
```

For security reasons, you cannot delete a specific trace or dump file on a SQL Server DB instance. To delete all unused trace or dump files, set the retention period for the files to 0.

Amazon RDS for MySQL

Amazon RDS supports DB instances that run the following versions of MySQL:

- MySQL 8.0
- MySQL 5.7

For more information about minor version support, see [MySQL on Amazon RDS versions \(p. 1315\)](#).

To create an Amazon RDS for MySQL DB instance, use the Amazon RDS management tools or interfaces. You can then do the following:

- Resize your DB instance
- Authorize connections to your DB instance
- Create and restore from backups or snapshots
- Create Multi-AZ secondaries
- Create read replicas
- Monitor the performance of your DB instance

To store and access the data in your DB instance, you use standard MySQL utilities and applications.

Amazon RDS for MySQL is compliant with many industry standards. For example, you can use RDS for MySQL databases to build HIPAA-compliant applications. You can use RDS for MySQL databases to store healthcare related information, including protected health information (PHI) under a Business Associate Agreement (BAA) with AWS. Amazon RDS for MySQL also meets Federal Risk and Authorization Management Program (FedRAMP) security requirements. In addition, Amazon RDS for MySQL has received a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the FedRAMP HIGH Baseline within the AWS GovCloud (US) Regions. For more information on supported compliance standards, see [AWS cloud compliance](#).

For information about the features in each version of MySQL, see [The main features of MySQL](#) in the MySQL documentation.

Before creating a DB instance, complete the steps in [Setting up for Amazon RDS \(p. 148\)](#). When you create a DB instance, the RDS master user gets DBA privileges, with some limitations. Use this account for administrative tasks such as creating additional database accounts.

You can create the following:

- DB instances
- DB snapshots
- Point-in-time restores
- Automated backups
- Manual backups

You can use DB instances running MySQL inside a virtual private cloud (VPC) based on Amazon VPC. You can also add features to your MySQL DB instance by turning on various options. Amazon RDS supports Multi-AZ deployments for MySQL as a high-availability, failover solution.

Important

To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. It also restricts access to certain system procedures and tables that need advanced

privileges. You can access your database using standard SQL clients such as the mysql client. However, you can't access the host directly by using Telnet or Secure Shell (SSH).

Topics

- [MySQL feature support on Amazon RDS \(p. 1312\)](#)
- [MySQL on Amazon RDS versions \(p. 1315\)](#)
- [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#)
- [Securing MySQL DB instance connections \(p. 1325\)](#)
- [Upgrading the MySQL DB engine \(p. 1343\)](#)
- [Upgrading a MySQL DB snapshot \(p. 1353\)](#)
- [Importing data into a MySQL DB instance \(p. 1355\)](#)
- [Working with MySQL replication in Amazon RDS \(p. 1389\)](#)
- [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#)
- [Options for MySQL DB instances \(p. 1416\)](#)
- [Parameters for MySQL \(p. 1426\)](#)
- [Common DBA tasks for MySQL DB instances \(p. 1428\)](#)
- [Local time zone for MySQL DB instances \(p. 1433\)](#)
- [Known issues and limitations for Amazon RDS for MySQL \(p. 1435\)](#)
- [MySQL on Amazon RDS SQL reference \(p. 1439\)](#)

MySQL feature support on Amazon RDS

RDS for MySQL supports most of the features and capabilities of MySQL. Some features might have limited support or restricted privileges.

You can filter new Amazon RDS features on the [What's New with Database?](#) page. For **Products**, choose **Amazon RDS**. Then search using keywords such as **MySQL 2022**.

Note

The following lists are not exhaustive.

Topics

- [Supported storage engines for RDS for MySQL \(p. 1312\)](#)
- [Using memcached and other options with MySQL on Amazon RDS \(p. 1312\)](#)
- [InnoDB cache warming for MySQL on Amazon RDS \(p. 1313\)](#)
- [MySQL features not supported by Amazon RDS \(p. 1313\)](#)

Supported storage engines for RDS for MySQL

While MySQL supports multiple storage engines with varying capabilities, not all of them are optimized for recovery and data durability. Amazon RDS fully supports the InnoDB storage engine for MySQL DB instances. Amazon RDS features such as Point-In-Time restore and snapshot restore require a recoverable storage engine and are supported for the InnoDB storage engine only. For more information, see [MySQL memcached support \(p. 1422\)](#).

The Federated Storage Engine is currently not supported by Amazon RDS for MySQL.

For user-created schemas, the MyISAM storage engine does not support reliable recovery and can result in lost or corrupt data when MySQL is restarted after a recovery, preventing Point-In-Time restore or snapshot restore from working as intended. However, if you still choose to use MyISAM with Amazon RDS, snapshots can be helpful under some conditions.

Note

System tables in the mysql schema can be in MyISAM storage.

If you want to convert existing MyISAM tables to InnoDB tables, you can use the `ALTER TABLE` command (for example, `alter table TABLE_NAME engine=innodb;`). Bear in mind that MyISAM and InnoDB have different strengths and weaknesses, so you should fully evaluate the impact of making this switch on your applications before doing so.

MySQL 5.1, 5.5, and 5.6 are no longer supported in Amazon RDS. However, you can restore existing MySQL 5.1, 5.5, and 5.6 snapshots. When you restore a MySQL 5.1, 5.5, or 5.6 snapshot, the DB instance is automatically upgraded to MySQL 5.7.

Using memcached and other options with MySQL on Amazon RDS

Most Amazon RDS DB engines support option groups that allow you to select additional features for your DB instance. RDS for MySQL DB instances support the memcached option, a simple, key-based cache. For more information about memcached and other options, see [Options for MySQL DB instances \(p. 1416\)](#). For more information about working with option groups, see [Working with option groups \(p. 273\)](#).

InnoDB cache warming for MySQL on Amazon RDS

InnoDB cache warming can provide performance gains for your MySQL DB instance by saving the current state of the buffer pool when the DB instance is shut down, and then reloading the buffer pool from the saved information when the DB instance starts up. This bypasses the need for the buffer pool to "warm up" from normal database use and instead preloads the buffer pool with the pages for known common queries. The file that stores the saved buffer pool information only stores metadata for the pages that are in the buffer pool, and not the pages themselves. As a result, the file does not require much storage space. The file size is about 0.2 percent of the cache size. For example, for a 64 GiB cache, the cache warming file size is 128 MiB. For more information on InnoDB cache warming, see [Saving and restoring the buffer pool state](#) in the MySQL documentation.

RDS for MySQL DB instances support InnoDB cache warming. To enable InnoDB cache warming, set the `innodb_buffer_pool_dump_at_shutdown` and `innodb_buffer_pool_load_at_startup` parameters to 1 in the parameter group for your DB instance. Changing these parameter values in a parameter group will affect all MySQL DB instances that use that parameter group. To enable InnoDB cache warming for specific MySQL DB instances, you might need to create a new parameter group for those instances. For information on parameter groups, see [Working with parameter groups \(p. 289\)](#).

InnoDB cache warming primarily provides a performance benefit for DB instances that use standard storage. If you use PIOPS storage, you do not commonly see a significant performance benefit.

Important

If your MySQL DB instance does not shut down normally, such as during a failover, then the buffer pool state will not be saved to disk. In this case, MySQL loads whatever buffer pool file is available when the DB instance is restarted. No harm is done, but the restored buffer pool might not reflect the most recent state of the buffer pool prior to the restart. To ensure that you have a recent state of the buffer pool available to warm the InnoDB cache on startup, we recommend that you periodically dump the buffer pool "on demand."

You can create an event to dump the buffer pool automatically and on a regular interval. For example, the following statement creates an event named `periodic_buffer_pool_dump` that dumps the buffer pool every hour.

```
CREATE EVENT periodic_buffer_pool_dump
ON SCHEDULE EVERY 1 HOUR
DO CALL mysql.rds_innodb_buffer_pool_dump_now();
```

For more information on MySQL events, see [Event syntax](#) in the MySQL documentation.

Dumping and loading the buffer pool on demand

You can save and load the InnoDB cache "on demand."

- To dump the current state of the buffer pool to disk, call the [mysql.rds_innodb_buffer_pool_dump_now \(p. 1458\)](#) stored procedure.
- To load the saved state of the buffer pool from disk, call the [mysql.rds_innodb_buffer_pool_load_now \(p. 1458\)](#) stored procedure.
- To cancel a load operation in progress, call the [mysql.rds_innodb_buffer_pool_load_abort \(p. 1459\)](#) stored procedure.

MySQL features not supported by Amazon RDS

Amazon RDS doesn't currently support the following MySQL features:

- Authentication Plugin

- Error Logging to the System Log
- Group Replication Plugin
- InnoDB Tablespace Encryption
- Password Strength Plugin
- Persisted system variables
- Rewriter Query Rewrite Plugin
- Semisynchronous replication
- Transportable tablespace
- X Plugin

Note

Global transaction IDs are supported for all RDS for MySQL 5.7 versions, and for RDS for MySQL 8.0.26 and higher 8.0 versions.

To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. It also restricts access to certain system procedures and tables that require advanced privileges. Amazon RDS supports access to databases on a DB instance using any standard SQL client application. Amazon RDS doesn't allow direct host access to a DB instance by using Telnet, Secure Shell (SSH), or Windows Remote Desktop Connection. When you create a DB instance, you are assigned to the *db_owner* role for all databases on that instance, and you have all database-level permissions except for those used for backups. Amazon RDS manages backups for you.

MySQL on Amazon RDS versions

For MySQL, version numbers are organized as version = X.Y.Z. In Amazon RDS terminology, X.Y denotes the major version, and Z is the minor version number. For Amazon RDS implementations, a version change is considered major if the major version number changes—for example, going from version 5.7 to 8.0. A version change is considered minor if only the minor version number changes—for example, going from version 8.0.27 to 8.0.30.

Topics

- [Supported MySQL versions on Amazon RDS \(p. 1315\)](#)
- [RDS for MySQL release calendar \(p. 1316\)](#)
- [Deprecated versions for Amazon RDS for MySQL \(p. 1317\)](#)

Supported MySQL versions on Amazon RDS

Amazon RDS currently supports the following versions of MySQL:

Major version	Minor version
MySQL 8.0	<ul style="list-style-type: none">• 8.0.31• 8.0.30• 8.0.28• 8.0.27• 8.0.26• 8.0.25• 8.0.23
MySQL 5.7	<ul style="list-style-type: none">• 5.7.40• 5.7.39• 5.7.38• 5.7.37• 5.7.34• 5.7.33

You can specify any currently supported MySQL version when creating a new DB instance. You can specify the major version (such as MySQL 5.7), and any supported minor version for the specified major version. If no version is specified, Amazon RDS defaults to a supported version, typically the most recent version. If a major version is specified but a minor version is not, Amazon RDS defaults to a recent release of the major version you have specified. To see a list of supported versions, as well as defaults for newly created DB instances, use the [describe-db-engine-versions](#) AWS CLI command.

For example, to list the supported engine versions for RDS for MySQL, run the following CLI command:

```
aws rds describe-db-engine-versions --engine mysql --query "*[].\n{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

The default MySQL version might vary by AWS Region. To create a DB instance with a specific minor version, specify the minor version during DB instance creation. You can determine the default minor version for an AWS Region using the following AWS CLI command:

```
aws rds describe-db-engine-versions --default-only --engine mysql --engine-version major-engine-version --region region --query "*[].[Engine:Engine,EngineVersion:EngineVersion]" --output text
```

Replace *major-engine-version* with the major engine version, and replace *region* with the AWS Region. For example, the following AWS CLI command returns the default MySQL minor engine version for the 5.7 major version and the US West (Oregon) AWS Region (us-west-2):

```
aws rds describe-db-engine-versions --default-only --engine mysql --engine-version 5.7 --region us-west-2 --query "*[].[Engine:Engine,EngineVersion:EngineVersion]" --output text
```

With Amazon RDS, you control when to upgrade your MySQL instance to a new major version supported by Amazon RDS. You can maintain compatibility with specific MySQL versions, test new versions with your application before deploying in production, and perform major version upgrades at times that best fit your schedule.

When automatic minor version upgrade is enabled, your DB instance will be upgraded automatically to new MySQL minor versions as they are supported by Amazon RDS. This patching occurs during your scheduled maintenance window. You can modify a DB instance to enable or disable automatic minor version upgrades.

If you opt out of automatically scheduled upgrades, you can manually upgrade to a supported minor version release by following the same procedure as you would for a major version update. For information, see [Upgrading a DB instance engine version \(p. 360\)](#).

Amazon RDS currently supports the major version upgrades from MySQL version 5.6 to version 5.7, and from MySQL version 5.7 to version 8.0. Because major version upgrades involve some compatibility risk, they do not occur automatically; you must make a request to modify the DB instance. You should thoroughly test any upgrade before upgrading your production instances. For information about upgrading a MySQL DB instance, see [Upgrading the MySQL DB engine \(p. 1343\)](#).

You can test a DB instance against a new version before upgrading by creating a DB snapshot of your existing DB instance, restoring from the DB snapshot to create a new DB instance, and then initiating a version upgrade for the new DB instance. You can then experiment safely on the upgraded clone of your DB instance before deciding whether or not to upgrade your original DB instance.

RDS for MySQL release calendar

RDS for MySQL major versions remain available at least until community end of life for the corresponding community version. You can use the following dates to plan your testing and upgrade cycles. If Amazon extends support for an RDS for MySQL version for longer than originally stated, we plan to update this table to reflect the later date.

Note

Dates with only a month and a year are approximate and are updated with an exact date when it's known.

MySQL major version	Community release date	RDS release date	Community end of life date	RDS end of standard support date
MySQL 8.0 Current minor version: 8.0.31	19 April 2018	23 October 2018	April 2026	April 2026

MySQL major version	Community release date	RDS release date	Community end of life date	RDS end of standard support date
MySQL 5.7 Current minor version: 5.7.40	21 October 2015	22 February 2016	October 2023	October 2023
MySQL 5.6 Current minor version: N/A	5 February 2013	1 July 2013	5 February 2021	1 March 2022

Deprecated versions for Amazon RDS for MySQL

Amazon RDS for MySQL version 5.1, 5.5, and 5.6 are deprecated.

For information about the Amazon RDS deprecation policy for MySQL, see [Amazon RDS FAQs](#).

Connecting to a DB instance running the MySQL database engine

Before you can connect to a DB instance running the MySQL database engine, you must create a DB instance. For information, see [Creating an Amazon RDS DB instance \(p. 230\)](#). After Amazon RDS provisions your DB instance, you can use any standard MySQL client application or utility to connect to the instance. In the connection string, you specify the DNS address from the DB instance endpoint as the host parameter, and specify the port number from the DB instance endpoint as the port parameter.

To authenticate to your RDS DB instance, you can use one of the authentication methods for MySQL and AWS Identity and Access Management (IAM) database authentication:

- To learn how to authenticate to MySQL using one of the authentication methods for MySQL, see [Authentication method](#) in the MySQL documentation.
- To learn how to authenticate to MySQL using IAM database authentication, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

You can connect to a MySQL DB instance by using tools like the MySQL command-line client. For more information on using the MySQL command-line client, see [mysql – the MySQL command-line client](#) in the MySQL documentation. One GUI-based application you can use to connect is MySQL Workbench. For more information, see the [Download MySQL Workbench](#) page. For information about installing MySQL (including the MySQL command-line client), see [Installing and upgrading MySQL](#).

Most Linux distributions include the MariaDB client instead of the Oracle MySQL client. To install the MySQL command-line client on most RPM-based Linux distributions, including Amazon Linux 2, run the following command:

```
yum install mariadb
```

To install the MySQL command-line client on most DEB-based Linux distributions, run the following command:

```
apt-get install mariadb-client
```

To check the version of your MySQL command-line client, run the following command:

```
mysql --version
```

To read the MySQL documentation for your current client version, run the following command:

```
man mysql
```

To connect to a DB instance from outside of its Amazon VPC, the DB instance must be publicly accessible, access must be granted using the inbound rules of the DB instance's security group, and other requirements must be met. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

You can use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption on connections to a MySQL DB instance. For information, see [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#). If you are using AWS Identity and Access Management (IAM) database authentication, make sure to use an SSL/TLS connection. For information, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

You can also connect to a DB instance from a web server. For more information, see [Tutorial: Create a web server and an Amazon RDS DB instance \(p. 198\)](#).

Note

For information on connecting to a MariaDB DB instance, see [Connecting to a DB instance running the MariaDB database engine \(p. 986\)](#).

Topics

- [Finding the connection information for a MySQL DB instance \(p. 1319\)](#)
- [Connecting from the MySQL command-line client \(unencrypted\) \(p. 1321\)](#)
- [Connecting from MySQL Workbench \(p. 1322\)](#)
- [Connecting with the Amazon Web Services JDBC Driver for MySQL \(p. 1323\)](#)
- [Troubleshooting connections to your MySQL DB instance \(p. 1324\)](#)

Finding the connection information for a MySQL DB instance

The connection information for a DB instance includes its endpoint, port, and a valid database user, such as the master user. For example, suppose that an endpoint value is mydb.123456789012.us-east-1.rds.amazonaws.com. In this case, the port value is 3306, and the database user is admin. Given this information, you specify the following values in a connection string:

- For host or host name or DNS name, specify mydb.123456789012.us-east-1.rds.amazonaws.com.
- For port, specify 3306.
- For user, specify admin.

To connect to a DB instance, use any client for the MySQL DB engine. For example, you might use the MySQL command-line client or MySQL Workbench.

To find the connection information for a DB instance, you can use the AWS Management Console, the AWS CLI [describe-db-instances](#) command, or the Amazon RDS API [DescribeDBInstances](#) operation to list its details.

Console

To find the connection information for a DB instance in the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases** to display a list of your DB instances.
3. Choose the name of the MySQL DB instance to display its details.
4. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the Amazon RDS console interface. At the top, the navigation path is "RDS > Databases > mydb". Below this, the database name "mydb" is displayed in large text. A "Summary" section provides basic information: DB identifier (mydb), Role (Instance), CPU usage (2.33%), and Current activity (0 Connections). Below the summary is a tab bar with "Connectivity & security" (highlighted in orange), "Monitoring", "Logs & events", and "Configuration". The "Connectivity & security" section displays the endpoint and port details, which are circled in red.

Endpoint	Port	Network
mydb. [REDACTED].us-east-1.rds.amazonaws.com	3306	Available
		VPC
		vpc-6E
		Subnet
		default

5. If you need to find the master user name, choose the **Configuration** tab and view the **Master username** value.

AWS CLI

To find the connection information for a MySQL DB instance by using the AWS CLI, call the [describe-db-instances](#) command. In the call, query for the DB instance ID, endpoint, port, and master user name.

For Linux, macOS, or Unix:

```
aws rds describe-db-instances \
--filters "Name=engine,Values=mysql" \
--query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

For Windows:

```
aws rds describe-db-instances ^
--filters "Name=engine,Values=mysql" ^
--query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

Your output should be similar to the following.

```
[  
  [  
    "mydb1",  
    "mydb1.123456789012.us-east-1.rds.amazonaws.com",  
    3306,  
    "admin"  
  ],  
  [  
    "mydb2",  
    "mydb2.123456789012.us-east-1.rds.amazonaws.com",  
    3306,  
    "admin"  
  ]  
]
```

RDS API

To find the connection information for a DB instance by using the Amazon RDS API, call the [DescribeDBInstances](#) operation. In the output, find the values for the endpoint address, endpoint port, and master user name.

Connecting from the MySQL command-line client (unencrypted)

Important

Only use an unencrypted MySQL connection when the client and server are in the same VPC and the network is trusted. For information about using encrypted connections, see [Connecting from the MySQL command-line client with SSL/TLS \(encrypted\) \(p. 1328\)](#).

To connect to a DB instance using the MySQL command-line client, enter the following command at the command prompt. For the -h parameter, substitute the DNS name (endpoint) for your DB instance. For the -P parameter, substitute the port for your DB instance. For the -u parameter, substitute the user name of a valid database user, such as the master user. Enter the master user password when prompted.

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com -P 3306 -u mymasteruser -p
```

After you enter the password for the user, you should see output similar to the following.

```
Welcome to the MySQL monitor. Commands end with ; or \g.
```

```
Your MySQL connection id is 9738
Server version: 8.0.23 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Connecting from MySQL Workbench

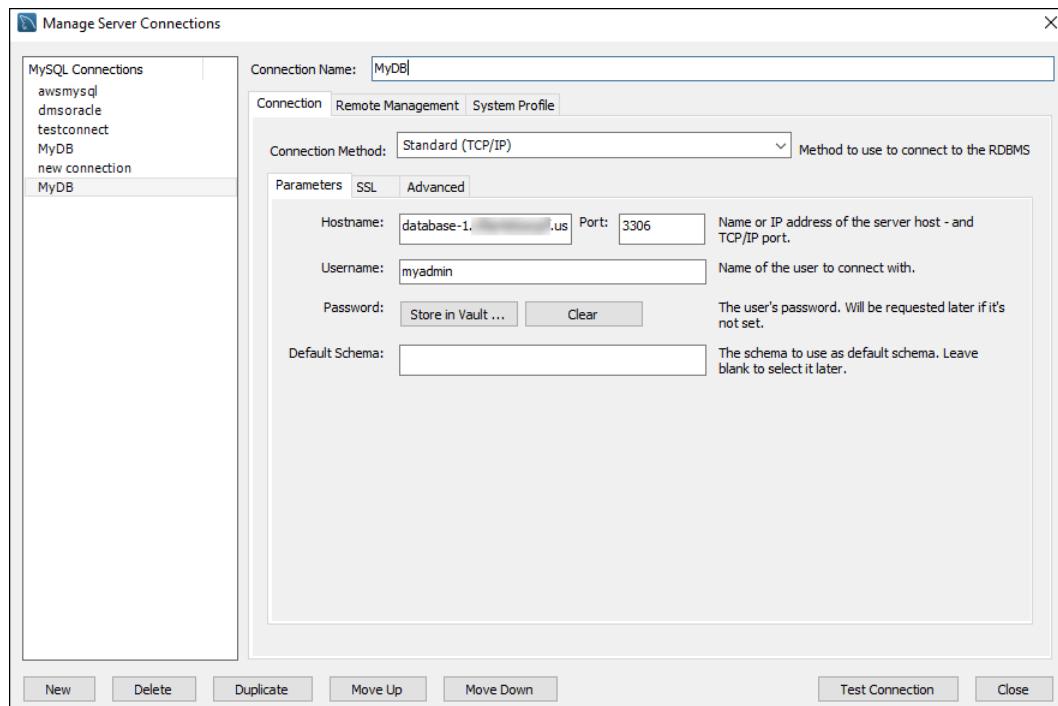
To connect from MySQL Workbench

1. Download and install MySQL Workbench at [Download MySQL Workbench](#).
2. Open MySQL Workbench.



3. From **Database**, choose **Manage Connections**.
4. In the **Manage Server Connections** window, choose **New**.
5. In the **Connect to Database** window, enter the following information:
 - **Stored Connection** – Enter a name for the connection, such as **MyDB**.
 - **Hostname** – Enter the DB instance endpoint.
 - **Port** – Enter the port used by the DB instance.
 - **Username** – Enter the user name of a valid database user, such as the master user.
 - **Password** – Optionally, choose **Store in Vault** and then enter and save the password for the user.

The window looks similar to the following:



You can use the features of MySQL Workbench to customize connections. For example, you can use the **SSL** tab to configure SSL/TLS connections. For information about using MySQL Workbench, see the [MySQL Workbench documentation](#). Encrypting client connections to MySQL DB instances with SSL/TLS, see [Encrypting client connections to MySQL DB instances with SSL/TLS \(p. 1327\)](#).

6. Optionally, choose **Test Connection** to confirm that the connection to the DB instance is successful.
7. Choose **Close**.
8. From **Database**, choose **Connect to Database**.
9. From **Stored Connection**, choose your connection.
10. Choose **OK**.

Connecting with the Amazon Web Services JDBC Driver for MySQL

The AWS JDBC Driver for MySQL is a client driver designed for RDS for MySQL. By default, the driver has settings that are optimized for use with RDS for MySQL. For more information about the driver and complete instructions for using it, see [the AWS JDBC Driver for MySQL GitHub repository](#).

The driver is drop-in compatible with the MySQL Connector/J driver. To install or upgrade your connector, replace the MySQL connector .jar file (located in the application CLASSPATH) with the AWS JDBC Driver for MySQL .jar file, and update the connection URL prefix from `jdbc:mysql://` to `jdbc:mysql:aws://`.

The AWS JDBC Driver for MySQL supports IAM database authentication. For more information, see [AWS IAM Database Authentication](#) in the AWS JDBC Driver for MySQL GitHub repository. For more information about IAM database authentication, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

Troubleshooting connections to your MySQL DB instance

Two common causes of connection failures to a new DB instance are:

- The DB instance was created using a security group that doesn't authorize connections from the device or Amazon EC2 instance where the MySQL application or utility is running. The DB instance must have a VPC security group that authorizes the connections. For more information, see [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#).

You can add or edit an inbound rule in the security group. For **Source**, choose **My IP**. This allows access to the DB instance from the IP address detected in your browser.

- The DB instance was created using the default port of 3306, and your company has firewall rules blocking connections to that port from devices in your company network. To fix this failure, recreate the instance with a different port.

For more information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Securing MySQL DB instance connections

You can manage the security of your MySQL DB instances.

Topics

- [MySQL security on Amazon RDS \(p. 1325\)](#)
- [Using the Password Validation Plugin for RDS for MySQL \(p. 1326\)](#)
- [Encrypting client connections to MySQL DB instances with SSL/TLS \(p. 1327\)](#)
- [Using new SSL/TLS certificates for MySQL DB instances \(p. 1330\)](#)
- [Using Kerberos authentication for MySQL \(p. 1333\)](#)

MySQL security on Amazon RDS

Security for MySQL DB instances is managed at three levels:

- AWS Identity and Access Management controls who can perform Amazon RDS management actions on DB instances. When you connect to AWS using IAM credentials, your IAM account must have IAM policies that grant the permissions required to perform Amazon RDS management operations. For more information, see [Identity and access management for Amazon RDS \(p. 2016\)](#).
- When you create a DB instance, you use a VPC security group to control which devices and Amazon EC2 instances can open connections to the endpoint and port of the DB instance. These connections can be made using Secure Sockets Layer (SSL) and Transport Layer Security (TLS). In addition, firewall rules at your company can control whether devices running at your company can open connections to the DB instance.
- To authenticate login and permissions for a MySQL DB instance, you can take either of the following approaches, or a combination of them.

You can take the same approach as with a stand-alone instance of MySQL. Commands such as CREATE USER, RENAME USER, GRANT, REVOKE, and SET PASSWORD work just as they do in on-premises databases, as does directly modifying database schema tables. For information, see [Access control and account management](#) in the MySQL documentation.

You can also use IAM database authentication. With IAM database authentication, you authenticate to your DB instance by using an IAM user or IAM role and an authentication token. An *authentication token* is a unique value that is generated using the Signature Version 4 signing process. By using IAM database authentication, you can use the same credentials to control access to your AWS resources and your databases. For more information, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

Another option is Kerberos authentication for RDS for MySQL. The DB instance works with AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to enable Kerberos authentication. When users authenticate with a MySQL DB instance joined to the trusting domain, authentication requests are forwarded. Forwarded requests go to the domain directory that you create with AWS Directory Service. For more information, see [Using Kerberos authentication for MySQL \(p. 1333\)](#).

When you create an Amazon RDS DB instance, the master user has the following default privileges:

- alter
- alter routine
- create
- create routine

- create temporary tables
- create user
- create view
- delete
- drop
- event
- execute
- grant option
- index
- insert
- lock tables
- process
- references
- replication client
- replication slave
- select
- show databases
- show view
- trigger
- update

Note

Although it is possible to delete the master user on the DB instance, it is not recommended. To recreate the master user, use the [ModifyDBInstance](#) RDS API operation or the [modify-db-instance](#) AWS CLI command and specify a new master user password with the appropriate parameter. If the master user does not exist in the instance, the master user is created with the specified password.

To provide management services for each DB instance, the `rdsadmin` user is created when the DB instance is created. Attempting to drop, rename, change the password, or change privileges for the `rdsadmin` account will result in an error.

To allow management of the DB instance, the standard `kill` and `kill_query` commands have been restricted. The Amazon RDS commands `rds_kill` and `rds_kill_query` are provided to allow you to end user sessions or queries on DB instances.

Using the Password Validation Plugin for RDS for MySQL

MySQL provides the `validate_password` plugin for improved security. The plugin enforces password policies using parameters in the DB parameter group for your MySQL DB instance. The plugin is supported for DB instances running MySQL version 5.7 and 8.0. For more information about the `validate_password` plugin, see [The Password Validation Plugin](#) in the MySQL documentation.

To enable the `validate_password` plugin for a MySQL DB instance

1. Connect to your MySQL DB instance and run the following command.

```
INSTALL PLUGIN validate_password SONAME 'validate_password.so';
```

2. Configure the parameters for the plugin in the DB parameter group used by the DB instance.

For more information about the parameters, see [Password Validation Plugin options and variables](#) in the MySQL documentation.

For more information about modifying DB instance parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

After installing and enabling the `password_validate` plugin, reset existing passwords to comply with your new validation policies.

Amazon RDS doesn't validate passwords. The MySQL DB instance performs password validation. If you set a user password with the AWS Management Console, the `modify-db-instance` AWS CLI command, or the `ModifyDBInstance` RDS API operation, the change can succeed even if the new password doesn't satisfy your password policies. However, a new password is set in the MySQL DB instance only if it satisfies the password policies. In this case, Amazon RDS records the following event.

```
"RDS-EVENT-0067" - An attempt to reset the master password for the DB instance has failed.
```

For more information about Amazon RDS events, see [Working with Amazon RDS event notification \(p. 650\)](#).

Encrypting client connections to MySQL DB instances with SSL/TLS

Secure Sockets Layer (SSL) is an industry-standard protocol for securing network connections between client and server. After SSL version 3.0, the name was changed to Transport Layer Security (TLS). Amazon RDS supports SSL/TLS encryption for MySQL DB instances. Using SSL/TLS, you can encrypt a connection between your application client and your MySQL DB instance. SSL/TLS support is available in all AWS Regions for MySQL.

Topics

- [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#)
- [Requiring SSL/TLS for all connections to a MySQL DB instance \(p. 1328\)](#)
- [Connecting from the MySQL command-line client with SSL/TLS \(encrypted\) \(p. 1328\)](#)

Using SSL/TLS with a MySQL DB instance

Amazon RDS creates an SSL/TLS certificate and installs the certificate on the DB instance when Amazon RDS provisions the instance. These certificates are signed by a certificate authority. The SSL/TLS certificate includes the DB instance endpoint as the Common Name (CN) for the SSL/TLS certificate to guard against spoofing attacks.

An SSL/TLS certificate created by Amazon RDS is the trusted root entity and should work in most cases but might fail if your application does not accept certificate chains. If your application does not accept certificate chains, you might need to use an intermediate certificate to connect to your AWS Region. For example, you must use an intermediate certificate to connect to the AWS GovCloud (US) Regions using SSL/TLS.

For information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For more information about using SSL/TLS with MySQL, see [Using new SSL/TLS certificates for MySQL DB instances \(p. 1330\)](#).

MySQL uses OpenSSL for secure connections. Amazon RDS for MySQL supports Transport Layer Security (TLS) versions 1.0, 1.1, and 1.2. The following table shows the TLS support for MySQL versions.

MySQL version	TLS 1.0	TLS 1.1	TLS 1.2
MySQL 8.0	Supported for MySQL 8.0.27 and lower	Supported for MySQL 8.0.27 and lower	Supported
MySQL 5.7	Supported	Supported	Supported

You can require SSL/TLS connections for specific users accounts. For example, you can use one of the following statements, depending on your MySQL version, to require SSL/TLS connections on the user account `encrypted_user`.

To do so, use the following statement.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

For more information on SSL/TLS connections with MySQL, see the [Using encrypted connections](#) in the MySQL documentation.

Requiring SSL/TLS for all connections to a MySQL DB instance

You can require that all user connections to your MySQL DB instance use SSL/TLS by using the `require_secure_transport` parameter. By default, the `require_secure_transport` parameter is set to OFF. You can set the `require_secure_transport` parameter to ON to require SSL/TLS for connections to your DB instance.

You can set the `require_secure_transport` parameter value by updating the DB parameter group for your DB instance. You don't need to reboot your DB instance for the change to take effect.

When the `require_secure_transport` parameter is set to ON for a DB instance, a database client can connect to it if it can establish an encrypted connection. Otherwise, an error message similar to the following is returned to the client:

```
MySQL Error 3159 (HY000): Connections using insecure transport are prohibited while --require_secure_transport=ON.
```

For information about setting parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

For more information about the `require_secure_transport` parameter, see the [MySQL documentation](#).

Connecting from the MySQL command-line client with SSL/TLS (encrypted)

The `mysql` client program parameters are slightly different if you are using the MySQL 5.7 version, the MySQL 8.0 version, or the MariaDB version.

To find out which version you have, run the mysql command with the --version option. In the following example, the output shows that the client program is from MariaDB.

```
$ mysql --version
mysql Ver 15.1 Distrib 10.5.15-MariaDB, for osx10.15 (x86_64) using readline 5.1
```

Most Linux distributions, such as Amazon Linux, CentOS, SUSE, and Debian have replaced MySQL with MariaDB, and the mysql version in them is from MariaDB.

To connect to your DB instance using SSL/TLS, follow these steps:

To connect to a DB instance with SSL/TLS using the MySQL command-line client

1. Download a root certificate that works for all AWS Regions.

For information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

2. Use a MySQL command-line client to connect to a DB instance with SSL/TLS encryption. For the -h parameter, substitute the DNS name (endpoint) for your DB instance. For the --ssl-ca parameter, substitute the SSL/TLS certificate file name. For the -P parameter, substitute the port for your DB instance. For the -u parameter, substitute the user name of a valid database user, such as the master user. Enter the master user password when prompted.

The following example shows how to launch the client using the --ssl-ca parameter using the MySQL 5.7 client or later:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl-mode=REQUIRED -P 3306 -u myadmin -p
```

To require that the SSL/TLS connection verifies the DB instance endpoint against the endpoint in the SSL/TLS certificate, enter the following command:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl-mode=VERIFY_IDENTITY -P 3306 -u myadmin -p
```

The following example shows how to launch the client using the --ssl-ca parameter using the MariaDB client:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-
bundle.pem --ssl -P 3306 -u myadmin -p
```

3. Enter the master user password when prompted.

You will see output similar to the following.

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 9738
Server version: 8.0.23 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Using new SSL/TLS certificates for MySQL DB instances

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your RDS DB instances using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.

This topic can help you to determine whether any client applications use SSL/TLS to connect to your DB instances. If they do, you can further check whether those applications require certificate verification to connect.

Note

Some applications are configured to connect to MySQL DB instances only if they can successfully verify the certificate on the server. For such applications, you must update your client application trust stores to include the new CA certificates.

You can specify the following SSL modes: disabled, preferred, and required. When you use the preferred SSL mode and the CA certificate doesn't exist or isn't up to date, the connection falls back to not using SSL and connects without encryption.

Because these later versions use the OpenSSL protocol, an expired server certificate doesn't prevent successful connections unless the required SSL mode is specified.

We recommend avoiding preferred mode. In preferred mode, if the connection encounters an invalid certificate, it stops using encryption and proceeds unencrypted.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB instances. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see [Rotating your SSL/TLS certificate \(p. 2007\)](#). For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For information about using SSL/TLS with MySQL DB instances, see [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#).

Topics

- [Determining whether any applications are connecting to your MySQL DB instance using SSL \(p. 1330\)](#)
- [Determining whether a client requires certificate verification to connect \(p. 1331\)](#)
- [Updating your application trust store \(p. 1332\)](#)
- [Example Java code for establishing SSL connections \(p. 1332\)](#)

Determining whether any applications are connecting to your MySQL DB instance using SSL

If you are using Amazon RDS for MySQL version 5.7 or 8.0 and the Performance Schema is enabled, run the following query to check if connections are using SSL/TLS. For information about enabling the Performance Schema, see [Performance Schema quick start](#) in the MySQL documentation.

```
mysql> SELECT id, user, host, connection_type
    FROM performance_schema.threads pst
    INNER JOIN information_schema.processlist isp
    ON pst.processlist_id = isp.id;
```

In this sample output, you can see both your own session (`admin`) and an application logged in as `webapp1` are using SSL.

```
+---+-----+-----+-----+
| id | user           | host          | connection_type |
+---+-----+-----+-----+
| 8  | admin          | 10.0.4.249:42590 | SSL/TLS        |
| 4  | event_scheduler | localhost      | NULL          |
| 10 | webapp1        | 159.28.1.1:42189 | SSL/TLS        |
+---+-----+-----+-----+
3 rows in set (0.00 sec)
```

Determining whether a client requires certificate verification to connect

You can check whether JDBC clients and MySQL clients require certificate verification to connect.

JDBC

The following example with MySQL Connector/J 8.0 shows one way to check an application's JDBC connection properties to determine whether successful connections require a valid certificate. For more information on all of the JDBC connection options for MySQL, see [Configuration properties](#) in the MySQL documentation.

When using the MySQL Connector/J 8.0, an SSL connection requires verification against the server CA certificate if your connection properties have `sslMode` set to `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

Note

If you use either the MySQL Java Connector v5.1.38 or later, or the MySQL Java Connector v8.0.9 or later to connect to your databases, even if you haven't explicitly configured your applications to use SSL/TLS when connecting to your databases, these client drivers default to using SSL/TLS. In addition, when using SSL/TLS, they perform partial certificate verification and fail to connect if the database server certificate is expired.

MySQL

The following examples with the MySQL Client show two ways to check a script's MySQL connection to determine whether successful connections require a valid certificate. For more information on all of the connection options with the MySQL Client, see [Client-side configuration for encrypted connections](#) in the MySQL documentation.

When using the MySQL 5.7 or MySQL 8.0 Client, an SSL connection requires verification against the server CA certificate if for the `--ssl-mode` option you specify `VERIFY_CA` or `VERIFY_IDENTITY`, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --
ssl-mode=VERIFY_CA
```

When using the MySQL 5.6 Client, an SSL connection requires verification against the server CA certificate if you specify the `--ssl-verify-server-cert` option, as in the following example.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem --ssl-verify-server-cert
```

Updating your application trust store

For information about updating the trust store for MySQL applications, see [Installing SSL certificates](#) in the MySQL documentation.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

When you update the trust store, you can retain older certificates in addition to adding the new certificates.

If you are using the mysql JDBC driver in an application, set the following properties in the application.

```
System.setProperty("javax.net.ssl.trustStore", "certs");
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

When you start the application, set the following properties.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

Example Java code for establishing SSL connections

The following code example shows how to set up the SSL connection that validates the server certificate using JDBC.

```
public class MySQLSSLTest {

    private static final String DB_USER = "username";
    private static final String DB_PASSWORD = "password";
    // This key store has only the prod root ca.
    private static final String KEY_STORE_FILE_PATH = "file-path-to-keystore";
    private static final String KEY_STORE_PASS = "keystore-password";

    public static void test(String[] args) throws Exception {
        Class.forName("com.mysql.jdbc.Driver");

        System.setProperty("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        System.setProperty("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);

        Properties properties = new Properties();
        properties.setProperty("sslMode", "VERIFY_IDENTITY");
    }
}
```

```
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);

Connection connection = null;
Statement stmt = null;
ResultSet rs = null;
try {
    connection =
DriverManager.getConnection("jdbc:mysql://mydatabase.123456789012.us-east-1.rds.amazonaws.com:3306",properties);
    stmt = connection.createStatement();
    rs=stmt.executeQuery("SELECT 1 from dual");
} finally {
    if (rs != null) {
        try {
            rs.close();
        } catch (SQLException e) {
        }
    }
    if (stmt != null) {
        try {
            stmt.close();
        } catch (SQLException e) {
        }
    }
    if (connection != null) {
        try {
            connection.close();
        } catch (SQLException e) {
            e.printStackTrace();
        }
    }
}
return;
}
```

Important

After you have determined that your database connections use SSL/TLS and have updated your application trust store, you can update your database to use the rds-ca-2019 certificates. For instructions, see step 3 in [Updating your CA certificate by modifying your DB instance \(p. 2007\)](#).

Using Kerberos authentication for MySQL

You can use Kerberos authentication to authenticate users when they connect to your MySQL DB instance. The DB instance works with AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to enable Kerberos authentication. When users authenticate with a MySQL DB instance joined to the trusting domain, authentication requests are forwarded. Forwarded requests go to the domain directory that you create with AWS Directory Service.

Keeping all of your credentials in the same directory can save you time and effort. With this approach, you have a centralized place for storing and managing credentials for multiple DB instances. Using a directory can also improve your overall security profile.

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of Amazon RDS with Kerberos authentication, see [Kerberos authentication \(p. 101\)](#).

Overview of Setting up Kerberos authentication for MySQL DB instances

To set up Kerberos authentication for a MySQL DB instance, complete the following general steps, described in more detail later:

1. Use AWS Managed Microsoft AD to create an AWS Managed Microsoft AD directory. You can use the AWS Management Console, the AWS CLI, or the AWS Directory Service to create the directory. For details about doing so, see [Create your AWS Managed Microsoft AD directory](#) in the *AWS Directory Service Administration Guide*.
2. Create an AWS Identity and Access Management (IAM) role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`. The role allows Amazon RDS to make calls to your directory.

For the role to allow access, the AWS Security Token Service (AWS STS) endpoint must be activated in the AWS Region for your AWS account. AWS STS endpoints are active by default in all AWS Regions, and you can use them without any further actions. For more information, see [Activating and deactivating AWS STS in an AWS Region](#) in the *IAM User Guide*.

3. Create and configure users in the AWS Managed Microsoft AD directory using the Microsoft Active Directory tools. For more information about creating users in your Active Directory, see [Manage users and groups in AWS managed Microsoft AD](#) in the *AWS Directory Service Administration Guide*.
4. Create or modify a MySQL DB instance. If you use either the CLI or RDS API in the create request, specify a domain identifier with the `Domain` parameter. Use the `d-*` identifier that was generated when you created your directory and the name of the role that you created.

If you modify an existing MySQL DB instance to use Kerberos authentication, set the `domain` and `IAMRoleArn` parameters for the DB instance. Locate the DB instance in the same VPC as the domain directory.

5. Use the Amazon RDS master user credentials to connect to the MySQL DB instance. Create the user in MySQL using the `CREATE USER` clause `IDENTIFIED WITH 'auth_pam'`. Users that you create this way can log in to the MySQL DB instance using Kerberos authentication.

Setting up Kerberos authentication for MySQL DB instances

You use AWS Managed Microsoft AD to set up Kerberos authentication for a MySQL DB instance. To set up Kerberos authentication, you take the following steps.

Step 1: Create a directory using AWS Managed Microsoft AD

AWS Directory Service creates a fully managed Active Directory in the AWS Cloud. When you create an AWS Managed Microsoft AD directory, AWS Directory Service creates two domain controllers and Domain Name System (DNS) servers on your behalf. The directory servers are created in different subnets in a VPC. This redundancy helps make sure that your directory remains accessible even if a failure occurs.

When you create an AWS Managed Microsoft AD directory, AWS Directory Service performs the following tasks on your behalf:

- Sets up an Active Directory within the VPC.
- Creates a directory administrator account with the user name Admin and the specified password. You use this account to manage your directory.

Note

Be sure to save this password. AWS Directory Service doesn't store it. You can reset it, but you can't retrieve it.

- Creates a security group for the directory controllers.

When you launch an AWS Managed Microsoft AD, AWS creates an Organizational Unit (OU) that contains all of your directory's objects. This OU has the NetBIOS name that you typed when you created your directory and is located in the domain root. The domain root is owned and managed by AWS.

The Admin account that was created with your AWS Managed Microsoft AD directory has permissions for the most common administrative activities for your OU:

- Create, update, or delete users
- Add resources to your domain such as file or print servers, and then assign permissions for those resources to users in your OU
- Create additional OUs and containers
- Delegate authority
- Restore deleted objects from the Active Directory Recycle Bin
- Run AD and DNS Windows PowerShell modules on the Active Directory Web Service

The Admin account also has rights to perform the following domain-wide activities:

- Manage DNS configurations (add, remove, or update records, zones, and forwarders)
- View DNS event logs
- View security event logs

To create a directory with AWS Managed Microsoft AD

1. Sign in to the AWS Management Console and open the AWS Directory Service console at <https://console.aws.amazon.com/directorieservicev2/>.
2. In the navigation pane, choose **Directories** and choose **Set up Directory**.
3. Choose **AWS Managed Microsoft AD**. AWS Managed Microsoft AD is the only option that you can currently use with Amazon RDS.
4. Enter the following information:

Directory DNS name

The fully qualified name for the directory, such as **corp.example.com**.

Directory NetBIOS name

The short name for the directory, such as **CORP**.

Directory description

(Optional) A description for the directory.

Admin password

The password for the directory administrator. The directory creation process creates an administrator account with the user name Admin and this password.

The directory administrator password and can't include the word "admin." The password is case-sensitive and must be 8–64 characters in length. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a–z)
- Uppercase letters (A–Z)
- Numbers (0–9)
- Non-alphanumeric characters (~!@#\$%^&*_+=`|\{}{};:"'<,>,?./)

Confirm password

The administrator password retyped.

5. Choose **Next**.
6. Enter the following information in the **Networking** section and then choose **Next**:

VPC

The VPC for the directory. Create the MySQL DB instance in this same VPC.

Subnets

Subnets for the directory servers. The two subnets must be in different Availability Zones.

7. Review the directory information and make any necessary changes. When the information is correct, choose **Create directory**.

Review & create

Review

Directory type

Microsoft AD

VPC

vpc-8b6b78e9 ([REDACTED])

Directory DNS name

corp.example.com

Subnets

subnet-75128d10 ([REDACTED], us-east-1a)
subnet-f51665dd ([REDACTED], us-east-1b)

Directory NetBIOS name

CORP

Directory description

My directory

Pricing

Edition

Standard

Free trial eligible [Learn more](#)

30-day limited trial

~USD [REDACTED] *

* Includes two domain controllers, USD [REDACTED] /mo for each additional domain controller.

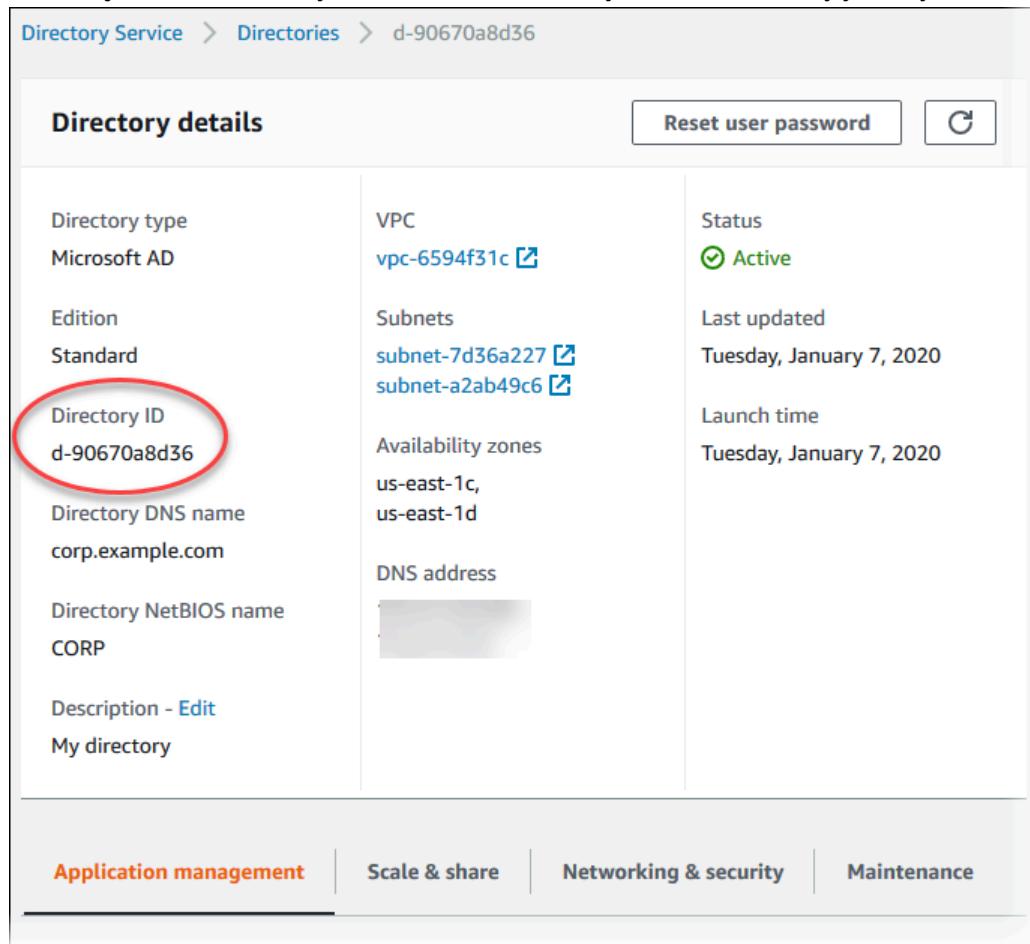
[Cancel](#)

[Previous](#)

[Create di](#)

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to **Active**.

To see information about your directory, choose the directory name in the directory listing. Note the **Directory ID** value because you need this value when you create or modify your MySQL DB instance.



The screenshot shows the 'Directory details' page for a Microsoft AD directory. The 'Directory ID' field, which contains the value 'd-90670a8d36', is circled in red. Other visible fields include 'Directory type' (Microsoft AD), 'Edition' (Standard), 'Status' (Active), 'Subnets' (subnet-7d36a227, subnet-a2ab49c6), 'Last updated' (Tuesday, January 7, 2020), 'Availability zones' (us-east-1c, us-east-1d), 'Launch time' (Tuesday, January 7, 2020), 'DNS address' (redacted), and a 'Description' field ('My directory'). Below the table, there are tabs for 'Application management' (which is selected), 'Scale & share', 'Networking & security', and 'Maintenance'.

Directory details		Reset user password	C
Directory type	VPC	Status	
Microsoft AD	vpc-6594f31c [edit]	Active	
Edition	Subnets	Last updated	
Standard	subnet-7d36a227 [edit] subnet-a2ab49c6 [edit]	Tuesday, January 7, 2020	
Directory ID	Availability zones	Launch time	
d-90670a8d36	us-east-1c, us-east-1d	Tuesday, January 7, 2020	
Directory DNS name	DNS address		
corp.example.com	[redacted]		
Directory NetBIOS name			
CORP			
Description - Edit			
My directory			

[Application management](#) | [Scale & share](#) | [Networking & security](#) | [Maintenance](#)

Step 2: Create the IAM role for use by Amazon RDS

For Amazon RDS to call AWS Directory Service for you, an IAM role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess` is required. This role allows Amazon RDS to make calls to the AWS Directory Service.

When a DB instance is created using the AWS Management Console and the console user has the `iam:CreateRole` permission, the console creates this role automatically. In this case, the role name is `rds-directoryservice-kerberos-access-role`. Otherwise, you must create the IAM role manually. When you create this IAM role, choose `Directory Service`, and attach the AWS managed policy `AmazonRDSDirectoryServiceAccess` to it.

For more information about creating IAM roles for a service, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Note

The IAM role used for Windows Authentication for RDS for SQL Server can't be used for RDS for MySQL.

Optionally, you can create policies with the required permissions instead of using the managed IAM policy `AmazonRDSDirectoryServiceAccess`. In this case, the IAM role must have the following IAM trust policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "directoryservice.rds.amazonaws.com",  
                    "rds.amazonaws.com"  
                ]  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

The role must also have the following IAM role policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ds:DescribeDirectories",  
                "ds:AuthorizeApplication",  
                "ds:UnauthorizeApplication",  
                "ds:GetAuthorizedApplicationDetails"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

Step 3: Create and configure users

You can create users with the Active Directory Users and Computers tool. This tool is part of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. Users represent individual people or entities that have access to your directory.

To create users in an AWS Directory Service directory, you must be connected to an Amazon EC2 instance based on Microsoft Windows. This instance must be a member of the AWS Directory Service directory and be logged in as a user that has privileges to create users. For more information, see [Manage users and groups in AWS Managed Microsoft AD](#) in the *AWS Directory Service Administration Guide*.

Step 4: Create or modify a MySQL DB instance

Create or modify a MySQL DB instance for use with your directory. You can use the console, CLI, or RDS API to associate a DB instance with a directory. You can do this in one of the following ways:

- Create a new MySQL DB instance using the console, the [create-db-instance](#) CLI command, or the [CreateDBInstance](#) RDS API operation.

For instructions, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

- Modify an existing MySQL DB instance using the console, the [modify-db-instance](#) CLI command, or the [ModifyDBInstance](#) RDS API operation.

For instructions, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- Restore a MySQL DB instance from a DB snapshot using the console, the [restore-db-instance-from-db-snapshot](#) CLI command, or the [RestoreDBInstanceFromDBSnapshot](#) RDS API operation.

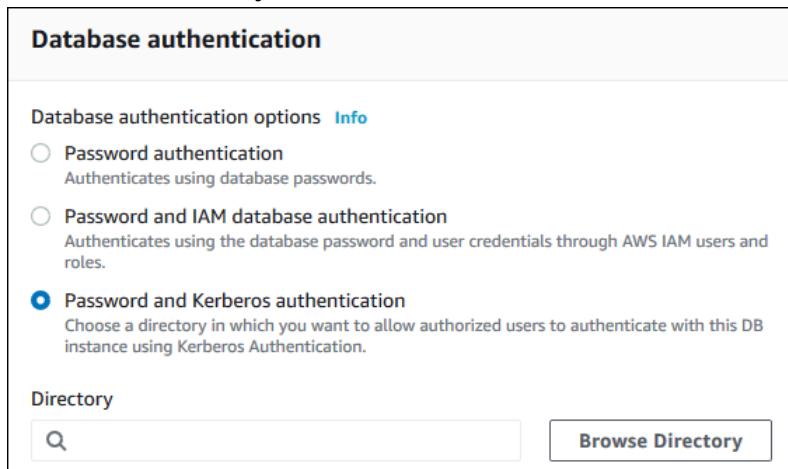
For instructions, see [Restoring from a DB snapshot \(p. 452\)](#).

- Restore a MySQL DB instance to a point-in-time using the console, the [restore-db-instance-to-point-in-time](#) CLI command, or the [RestoreDBInstanceToPointInTime](#) RDS API operation.

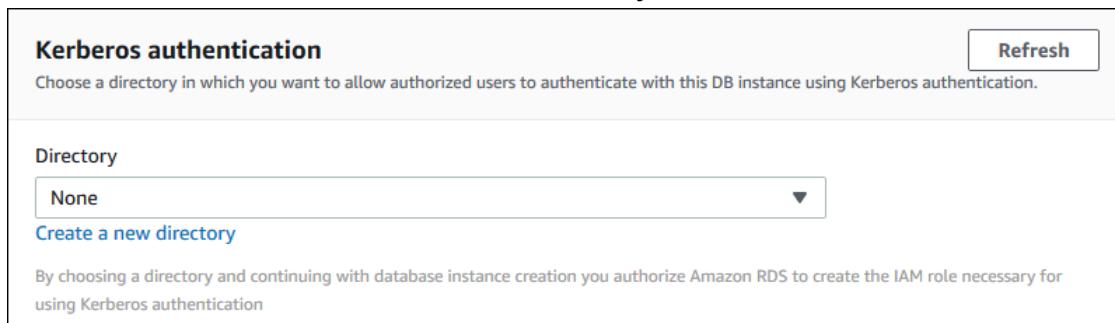
For instructions, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Kerberos authentication is only supported for MySQL DB instances in a VPC. The DB instance can be in the same VPC as the directory, or in a different VPC. The DB instance must use a security group that allows egress within the directory's VPC so the DB instance can communicate with the directory.

When you use the console to create a DB instance, choose **Password and Kerberos authentication** in the **Database authentication** section. Choose **Browse Directory** and then select the directory, or choose **Create a new directory**.



When you use the console to modify or restore a DB instance, choose the directory in the **Kerberos authentication** section, or choose **Create a new directory**.



Use the CLI or RDS API to associate a DB instance with a directory. The following parameters are required for the DB instance to be able to use the domain directory you created:

- For the `--domain` parameter, use the domain identifier ("d-*" identifier) generated when you created the directory.
- For the `--domain-iam-role-name` parameter, use the role you created that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

For example, the following CLI command modifies a DB instance to use a directory.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--domain d-ID \
--domain-iam-role-name role-name
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--domain d-ID ^
--domain-iam-role-name role-name
```

Important

If you modify a DB instance to enable Kerberos authentication, reboot the DB instance after making the change.

Step 5: Create Kerberos authentication MySQL logins

Use the Amazon RDS master user credentials to connect to the MySQL DB instance as you do any other DB instance. The DB instance is joined to the AWS Managed Microsoft AD domain. Thus, you can provision MySQL logins and users from the Active Directory users in your domain. Database permissions are managed through standard MySQL permissions that are granted to and revoked from these logins.

You can allow an Active Directory user to authenticate with MySQL. To do this, first use the Amazon RDS master user credentials to connect to the MySQL DB instance as with any other DB instance. After you're logged in, create an externally authenticated user with PAM (Pluggable Authentication Modules) in MySQL as shown following.

```
CREATE USER 'testuser'@'%' IDENTIFIED WITH 'auth_pam';
```

Replace *testuser* with the user name. Users (both humans and applications) from your domain can now connect to the DB instance from a domain joined client machine using Kerberos authentication.

Important

We strongly recommended that clients use SSL/TLS connections when using PAM authentication. If they don't use SSL/TLS connections, the password might be sent as clear text in some cases. To require an SSL/TLS encrypted connection for your AD user, run the following command:

```
UPDATE mysql.user SET ssl_type = 'any' WHERE ssl_type = '' AND PLUGIN = 'auth_pam' \
and USER = 'testuser'; \
FLUSH PRIVILEGES;
```

For more information, see [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#).

Managing a DB instance in a domain

You can use the CLI or the RDS API to manage your DB instance and its relationship with your managed Active Directory. For example, you can associate an Active Directory for Kerberos authentication and disassociate an Active Directory to disable Kerberos authentication. You can also move a DB instance to be externally authenticated by one Active Directory to another.

For example, using the Amazon RDS API, you can do the following:

- To reattempt enabling Kerberos authentication for a failed membership, use the `ModifyDBInstance` API operation and specify the current membership's directory ID.
- To update the IAM role name for membership, use the `ModifyDBInstance` API operation and specify the current membership's directory ID and the new IAM role.
- To disable Kerberos authentication on a DB instance, use the `ModifyDBInstance` API operation and specify none as the domain parameter.
- To move a DB instance from one domain to another, use the `ModifyDBInstance` API operation and specify the domain identifier of the new domain as the domain parameter.
- To list membership for each DB instance, use the `DescribeDBInstances` API operation.

Understanding domain membership

After you create or modify your DB instance, it becomes a member of the domain. You can view the status of the domain membership for the DB instance by running the `describe-db-instances` CLI command. The status of the DB instance can be one of the following:

- `kerberos-enabled` – The DB instance has Kerberos authentication enabled.
- `enabling-kerberos` – AWS is in the process of enabling Kerberos authentication on this DB instance.
- `pending-enable-kerberos` – The enabling of Kerberos authentication is pending on this DB instance.
- `pending-maintenance-enable-kerberos` – AWS will attempt to enable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `pending-disable-kerberos` – The disabling of Kerberos authentication is pending on this DB instance.
- `pending-maintenance-disable-kerberos` – AWS will attempt to disable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `enable-kerberos-failed` – A configuration problem has prevented AWS from enabling Kerberos authentication on the DB instance. Check and fix your configuration before reissuing the DB instance modify command.
- `disabling-kerberos` – AWS is in the process of disabling Kerberos authentication on this DB instance.

A request to enable Kerberos authentication can fail because of a network connectivity issue or an incorrect IAM role. For example, suppose that you create a DB instance or modify an existing DB instance and the attempt to enable Kerberos authentication fails. If this happens, re-issue the modify command or modify the newly created DB instance to join the domain.

Connecting to MySQL with Kerberos authentication

To connect to MySQL with Kerberos authentication, you must log in using the Kerberos authentication type.

To create a database user that you can connect to using Kerberos authentication, use an IDENTIFIED WITH clause on the `CREATE USER` statement. For instructions, see [Step 5: Create Kerberos authentication MySQL logins \(p. 1340\)](#).

To avoid errors, use the MariaDB `mysql` client. You can download MariaDB software at <https://downloads.mariadb.org/>.

At a command prompt, connect to one of the endpoints associated with your MySQL DB instance. Follow the general procedures in [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#). When you're prompted for the password, enter the Kerberos password associated with that user name.

Restoring a MySQL DB instance and adding it to a domain

You can restore a DB snapshot or complete a point-in-time restore for a MySQL DB instance and then add it to a domain. After the DB instance is restored, modify the DB instance using the process explained in [Step 4: Create or modify a MySQL DB instance \(p. 1338\)](#) to add the DB instance to a domain.

Kerberos authentication MySQL limitations

The following limitations apply to Kerberos authentication for MySQL:

- Only an AWS Managed Microsoft AD is supported. However, you can join RDS for MySQL DB instances to shared Managed Microsoft AD domains owned by different accounts in the same AWS Region.
- You must reboot the DB instance after enabling the feature.
- The domain name length can't be longer than 61 characters.
- You can't enable Kerberos authentication and IAM authentication at the same time. Choose one authentication method or the other for your MySQL DB instance.
- Don't modify the DB instance port after enabling the feature.
- Don't use Kerberos authentication with read replicas.
- If you have auto minor version upgrade turned on for a MySQL DB instance that is using Kerberos authentication, you must turn off Kerberos authentication and then turn it back on after an automatic upgrade. For more information about auto minor version upgrades, see [Automatic minor version upgrades for MySQL \(p. 1348\)](#).
- To delete a DB instance with this feature enabled, first disable the feature. To do this, use the `modify-db-instance` CLI command for the DB instance and specify `none` for the `--domain` parameter.

If you use the CLI or RDS API to delete a DB instance with this feature enabled, expect a delay.

Upgrading the MySQL DB engine

When Amazon RDS supports a new version of a database engine, you can upgrade your DB instances to the new version. There are two kinds of upgrades for MySQL DB instances: major version upgrades and minor version upgrades.

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, you must manually perform major version upgrades of your DB instances. You can initiate a major version upgrade by modifying your DB instance. However, before you perform a major version upgrade, we recommend that you follow the instructions in [Major version upgrades for MySQL \(p. 1344\)](#).

In contrast, *minor version upgrades* include only changes that are backward-compatible with existing applications. You can initiate a minor version upgrade manually by modifying your DB instance. Or you can enable the **Auto minor version upgrade** option when creating or modifying a DB instance. Doing so means that your DB instance is automatically upgraded after Amazon RDS tests and approves the new version. For information about performing an upgrade, see [Upgrading a DB instance engine version \(p. 360\)](#).

If your MySQL DB instance is using read replicas, you must upgrade all of the read replicas before upgrading the source instance. If your DB instance is in a Multi-AZ deployment, both the primary and standby replicas are upgraded. Your DB instance will not be available until the upgrade is complete.

Note

Database engine upgrades require downtime. The duration of the downtime varies based on the size of your DB instance.

Topics

- [Overview of upgrading \(p. 1343\)](#)
- [Major version upgrades for MySQL \(p. 1344\)](#)
- [Testing an upgrade \(p. 1348\)](#)
- [Upgrading a MySQL DB instance \(p. 1348\)](#)
- [Automatic minor version upgrades for MySQL \(p. 1348\)](#)
- [Using a read replica to reduce downtime when upgrading a MySQL database \(p. 1350\)](#)

Overview of upgrading

When you use the AWS Management Console to upgrade a DB instance, it shows the valid upgrade targets for the DB instance. You can also use the following AWS CLI command to identify the valid upgrade targets for a DB instance:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version version-number \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version version-number ^
```

```
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

For example, to identify the valid upgrade targets for a MySQL version 8.0.23 DB instance, run the following AWS CLI command:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \  
--engine mysql \  
--engine-version 8.0.23 \  
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^  
--engine mysql ^  
--engine-version 8.0.23 ^  
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --  
output text
```

Amazon RDS takes two DB snapshots during the upgrade process. The first DB snapshot is of the DB instance before any upgrade changes have been made. If the upgrade doesn't work for your databases, you can restore this snapshot to create a DB instance running the old version. The second DB snapshot is taken when the upgrade completes.

Note

Amazon RDS only takes DB snapshots if you have set the backup retention period for your DB instance to a number greater than 0. To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

After the upgrade is complete, you can't revert to the previous version of the database engine. If you want to return to the previous version, restore the first DB snapshot taken to create a new DB instance.

You control when to upgrade your DB instance to a new version supported by Amazon RDS. This level of control helps you maintain compatibility with specific database versions and test new versions with your application before deploying in production. When you are ready, you can perform version upgrades at the times that best fit your schedule.

If your DB instance is using read replication, you must upgrade all of the Read Replicas before upgrading the source instance.

If your DB instance is in a Multi-AZ deployment, both the primary and standby DB instances are upgraded. The primary and standby DB instances are upgraded at the same time and you will experience an outage until the upgrade is complete. The time for the outage varies based on your database engine, engine version, and the size of your DB instance.

Major version upgrades for MySQL

Amazon RDS supports the following in-place upgrades for major versions of the MySQL database engine:

- MySQL 5.6 to MySQL 5.7
- MySQL 5.7 to MySQL 8.0

Note

You can only create MySQL version 5.7 and 8.0 DB instances with latest-generation and current-generation DB instance classes, in addition to the db.m3 previous-generation DB instance class.

In some cases, you want to upgrade a MySQL version 5.6 DB instance running on a previous-generation DB instance class (other than db.m3) to a MySQL version 5.7 DB instance. In these cases, first modify the DB instance to use a latest-generation or current-generation DB instance class. After you do this, you can then modify the DB instance to use the MySQL version 5.7 database engine. For information on Amazon RDS DB instance classes, see [DB instance classes \(p. 10\)](#).

Topics

- [Overview of MySQL major version upgrades \(p. 1345\)](#)
- [Upgrades to MySQL version 5.7 might be slow \(p. 1345\)](#)
- [Prechecks for upgrades from MySQL 5.7 to 8.0 \(p. 1346\)](#)
- [Rollback after failure to upgrade from MySQL 5.7 to 8.0 \(p. 1347\)](#)

Overview of MySQL major version upgrades

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, Amazon RDS doesn't apply major version upgrades automatically; you must manually modify your DB instance. We recommend that you thoroughly test any upgrade before applying it to your production instances.

To perform a major version upgrade for a MySQL version 5.6 DB instance on Amazon RDS to MySQL version 5.7 or later, first perform any available OS updates. After OS updates are complete, upgrade to each major version: 5.6 to 5.7 and then 5.7 to 8.0. MySQL DB instances created before April 24, 2014, show an available OS update until the update has been applied. For more information on OS updates, see [Applying updates for a DB instance \(p. 352\)](#).

During a major version upgrade of MySQL, Amazon RDS runs the MySQL binary `mysql_upgrade` to upgrade tables, if necessary. Also, Amazon RDS empties the `slow_log` and `general_log` tables during a major version upgrade. To preserve log information, save the log contents before the major version upgrade.

MySQL major version upgrades typically complete in about 10 minutes. Some upgrades might take longer because of the DB instance class size or because the instance doesn't follow certain operational guidelines in [Best practices for Amazon RDS \(p. 216\)](#). If you upgrade a DB instance from the Amazon RDS console, the status of the DB instance indicates when the upgrade is complete. If you upgrade using the AWS Command Line Interface (AWS CLI), use the `describe-db-instances` command and check the `Status` value.

Upgrades to MySQL version 5.7 might be slow

MySQL version 5.6.4 introduced a new date and time format for the `datetime`, `time`, and `timestamp` columns that allows fractional components in date and time values. When upgrading a DB instance to MySQL version 5.7, MySQL forces the conversion of all date and time column types to the new format.

Because this conversion rebuilds your tables, it might take a considerable amount of time to complete the DB instance upgrade. The forced conversion occurs for any DB instances that are running a version before MySQL version 5.6.4. It also occurs for any DB instances that were upgraded from a version before MySQL version 5.6.4 to a version other than 5.7.

If your DB instance runs a version before MySQL version 5.6.4, or was upgraded from a version before 5.6.4, we recommend an extra step. In these cases, we recommend that you convert the `datetime`, `time`, and `timestamp` columns in your database before upgrading your DB instance to MySQL version 5.7. This conversion can significantly reduce the amount of time required to upgrade the DB instance to MySQL version 5.7. To upgrade your date and time columns to the new format, issue the `ALTER TABLE <table_name> FORCE`; command for each table that contains date or time columns. Because altering

a table locks the table as read-only, we recommend that you perform this update during a maintenance window.

To find all tables in your database that have `datetime`, `time`, or `timestamp` columns and create an `ALTER TABLE <table_name> FORCE`; command for each table, use the following query.

```
SET show_old_temporals = ON;
SELECT table_schema, table_name, column_name, column_type
FROM information_schema.columns
WHERE column_type LIKE '%/* 5.5 binary format */';
SET show_old_temporals = OFF;
```

Prechecks for upgrades from MySQL 5.7 to 8.0

MySQL 8.0 includes a number of incompatibilities with MySQL 5.7. These incompatibilities can cause problems during an upgrade from MySQL 5.7 to MySQL 8.0. So, some preparation might be required on your database for the upgrade to be successful. The following is a general list of these incompatibilities:

- There must be no tables that use obsolete data types or functions.
- There must be no orphan *.frm files.
- Triggers must not have a missing or empty definer or an invalid creation context.
- There must be no partitioned table that uses a storage engine that does not have native partitioning support.
- There must be no keyword or reserved word violations. Some keywords might be reserved in MySQL 8.0 that were not reserved previously.

For more information, see [Keywords and reserved words](#) in the MySQL documentation.

- There must be no tables in the MySQL 5.7 mysql system database that have the same name as a table used by the MySQL 8.0 data dictionary.
- There must be no obsolete SQL modes defined in your `sql_mode` system variable setting.
- There must be no tables or stored procedures with individual ENUM or SET column elements that exceed 255 characters or 1020 bytes in length.
- Before upgrading to MySQL 8.0.13 or higher, there must be no table partitions that reside in shared InnoDB tablespaces.
- There must be no queries and stored program definitions from MySQL 8.0.12 or lower that use ASC or DESC qualifiers for GROUP BY clauses.
- Your MySQL 5.7 installation must not use features that are not supported in MySQL 8.0.

For more information, see [Features removed in MySQL 8.0](#) in the MySQL documentation.

- There must be no foreign key constraint names longer than 64 characters.
- For improved Unicode support, consider converting objects that use the utf8mb3 charset to use the utf8mb4 charset. The utf8mb3 character set is deprecated. Also, consider using utf8mb4 for character set references instead of utf8, because currently utf8 is an alias for the utf8mb3 charset.

For more information, see [The utf8mb3 character set \(3-byte UTF-8 unicode encoding\)](#) in the MySQL documentation.

When you start an upgrade from MySQL 5.7 to 8.0, Amazon RDS runs prechecks automatically to detect these incompatibilities. For information about upgrading to MySQL 8.0, see [Upgrading MySQL](#) in the MySQL documentation.

These prechecks are mandatory. You can't choose to skip them. The prechecks provide the following benefits:

- They enable you to avoid unplanned downtime during the upgrade.
- If there are incompatibilities, Amazon RDS prevents the upgrade and provides a log for you to learn about them. You can then use the log to prepare your database for the upgrade to MySQL 8.0 by eliminating the incompatibilities. For detailed information about removing incompatibilities, see [Preparing your installation for upgrade](#) in the MySQL documentation and [Upgrading to MySQL 8.0? Here is what you need to know...](#) on the MySQL Server Blog.

The prechecks include some that are included with MySQL and some that were created specifically by the Amazon RDS team. For information about the prechecks provided by MySQL, see [Upgrade checker utility](#).

The prechecks run before the DB instance is stopped for the upgrade, meaning that they don't cause any downtime when they run. If the prechecks find an incompatibility, Amazon RDS automatically cancels the upgrade before the DB instance is stopped. Amazon RDS also generates an event for the incompatibility. For more information about Amazon RDS events, see [Working with Amazon RDS event notification \(p. 650\)](#).

Amazon RDS records detailed information about each incompatibility in the log file `PrePatchCompatibility.log`. In most cases, the log entry includes a link to the MySQL documentation for correcting the incompatibility. For more information about viewing log files, see [Viewing and listing database log files \(p. 680\)](#).

Due to the nature of the prechecks, they analyze the objects in your database. This analysis results in resource consumption and increases the time for the upgrade to complete.

Note

Amazon RDS runs all of these prechecks only for an upgrade from MySQL 5.7 to MySQL 8.0. For an upgrade from MySQL 5.6 to MySQL 5.7, prechecks are limited to confirming that there are no orphan tables and that there is enough storage space to rebuild tables. Prechecks aren't run for upgrades to releases lower than MySQL 5.7.

[Rollback after failure to upgrade from MySQL 5.7 to 8.0](#)

When you upgrade a DB instance from MySQL version 5.7 to MySQL version 8.0, the upgrade can fail. In particular, it can fail if the data dictionary contains incompatibilities that weren't captured by the prechecks. In this case, the database fails to start up successfully in the new MySQL 8.0 version. At this point, Amazon RDS rolls back the changes performed for the upgrade. After the rollback, the MySQL DB instance is running MySQL version 5.7. When an upgrade fails and is rolled back, Amazon RDS generates an event with the event ID RDS-EVENT-0188.

Typically, an upgrade fails because there are incompatibilities in the metadata between the databases in your DB instance and the target MySQL version. When an upgrade fails, you can view the details about these incompatibilities in the `upgradeFailure.log` file. Resolve the incompatibilities before attempting to upgrade again.

During an unsuccessful upgrade attempt and rollback, your DB instance is restarted. Any pending parameter changes are applied during the restart and persist after the rollback.

For more information about upgrading to MySQL 8.0, see the following topics in the MySQL documentation:

- [Preparing Your Installation for Upgrade](#)
- [Upgrading to MySQL 8.0? Here is what you need to know...](#)

Note

Currently, automatic rollback after upgrade failure is supported only for MySQL 5.7 to 8.0 major version upgrades.

Testing an upgrade

Before you perform a major version upgrade on your DB instance, thoroughly test your database for compatibility with the new version. In addition, thoroughly test all applications that access the database for compatibility with the new version. We recommend that you use the following procedure.

To test a major version upgrade

1. Review the upgrade documentation for the new version of the database engine to see if there are compatibility issues that might affect your database or applications:
 - [Changes in MySQL 5.6](#)
 - [Changes in MySQL 5.7](#)
 - [Changes in MySQL 8.0](#)
2. If your DB instance is a member of a custom DB parameter group, create a new DB parameter group with your existing settings that is compatible with the new major version. Specify the new DB parameter group when you upgrade your test instance, so your upgrade testing ensures that it works correctly. For more information about creating a DB parameter group, see [Working with parameter groups \(p. 289\)](#).
3. Create a DB snapshot of the DB instance to be upgraded. For more information, see [Creating a DB snapshot \(p. 448\)](#).
4. Restore the DB snapshot to create a new test DB instance. For more information, see [Restoring from a DB snapshot \(p. 452\)](#).
5. Modify this new test DB instance to upgrade it to the new version, using one of the methods detailed following. If you created a new parameter group in step 2, specify that parameter group.
6. Evaluate the storage used by the upgraded instance to determine if the upgrade requires additional storage.
7. Run as many of your quality assurance tests against the upgraded DB instance as needed to ensure that your database and application work correctly with the new version. Implement any new tests needed to evaluate the impact of any compatibility issues that you identified in step 1. Test all stored procedures and functions. Direct test versions of your applications to the upgraded DB instance.
8. If all tests pass, then perform the upgrade on your production DB instance. We recommend that you don't allow write operations to the DB instance until you confirm that everything is working correctly.

Upgrading a MySQL DB instance

For information about manually or automatically upgrading a MySQL DB instance, see [Upgrading a DB instance engine version \(p. 360\)](#).

Automatic minor version upgrades for MySQL

If you specify the following settings when creating or modifying a DB instance, you can have your DB instance automatically upgraded.

- The **Auto minor version upgrade** setting is enabled.
- The **Backup retention period** setting is greater than 0.

In the AWS Management Console, these settings are under **Additional configuration**. The following image shows the **Auto minor version upgrade** setting.

Maintenance

Auto minor version upgrade [Info](#)

Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)
Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Select window
 No preference

Start day	Start time	Duration
Monday	00 : 00 UTC	0.5 hours

For more information about these settings, see [Settings for DB instances \(p. 328\)](#).

For some RDS for MySQL major versions in some AWS Regions, one minor version is designated by RDS as the automatic upgrade version. After a minor version has been tested and approved by Amazon RDS, the minor version upgrade occurs automatically during your maintenance window. RDS doesn't automatically set newer released minor versions as the automatic upgrade version. Before RDS designates a newer automatic upgrade version, several criteria are considered, such as the following:

- Known security issues
- Bugs in the MySQL community version
- Overall fleet stability since the minor version was released

You can use the following AWS CLI command to determine the current automatic minor upgrade target version for a specified MySQL minor version in a specific AWS Region.

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

For example, the following AWS CLI command determines the automatic minor upgrade target for MySQL minor version 8.0.11 in the US East (Ohio) AWS Region (us-east-2).

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version 8.0.11 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version 8.0.11 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Your output is similar to the following.

DescribeDBEngineVersions	
AutoUpgrade	EngineVersion
False	8.0.15
False	8.0.16
False	8.0.17
False	8.0.19
False	8.0.20
False	8.0.21
True	8.0.23
False	8.0.25

In this example, the AutoUpgrade value is True for MySQL version 8.0.23. So, the automatic minor upgrade target is MySQL version 8.0.23, which is highlighted in the output.

A MySQL DB instance is automatically upgraded during your maintenance window if the following criteria are met:

- The **Auto minor version upgrade** setting is enabled.
- The **Backup retention period** setting is greater than 0.
- The DB instance is running a minor DB engine version that is less than the current automatic upgrade minor version.

For more information, see [Automatically upgrading the minor engine version \(p. 362\)](#).

Using a read replica to reduce downtime when upgrading a MySQL database

If your MySQL DB instance is currently in use with a production application, you can use the following procedure to upgrade the database version for your DB instance. This procedure can reduce the amount of downtime for your application.

By using a read replica, you can perform most of the maintenance steps ahead of time and minimize the necessary changes during the actual outage. With this technique, you can test and prepare the new DB instance without making any changes to your existing DB instance.

The following procedure shows an example of upgrading from MySQL version 5.7 to MySQL version 8.0. You can use the same general steps for upgrades to other major versions.

Note

When you are upgrading from MySQL version 5.7 to MySQL version 8.0, complete the prechecks before performing the upgrade. For more information, see [Prechecks for upgrades from MySQL 5.7 to 8.0 \(p. 1346\)](#).

To upgrade an MySQL database while a DB instance is in use

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Create a read replica of your MySQL 5.7 DB instance. This process creates an upgradable copy of your database. Other read replicas of the DB instance might also exist.
 - a. In the console, choose **Databases**, and then choose the DB instance that you want to upgrade.
 - b. For **Actions**, choose **Create read replica**.
 - c. Provide a value for **DB instance identifier** for your read replica and ensure that the **DB instance class** and other settings match your MySQL 5.7 DB instance.
 - d. Choose **Create read replica**.
3. (Optional) When the read replica has been created and **Status** shows **Available**, convert the read replica into a Multi-AZ deployment and enable backups.

By default, a read replicas is created as a single-AZ deployment with backups disabled. Because the read replica will ultimately become the production DB instance, it is a best practice to configure a Multi-AZ deployment and enable backups now.

- a. In the console, choose **Databases**, and then choose the read replica that you just created.
 - b. Choose **Modify**.
 - c. For **Multi-AZ deployment**, choose **Create a standby instance**.
 - d. For **Backup Retention Period**, choose a positive nonzero value, for example 3 days, and then choose **Continue**.
 - e. For **Scheduling of modifications**, choose **Apply immediately**.
 - f. Choose **Modify DB instance**.
4. When the read replica **Status** shows **Available**, upgrade the read replica to MySQL 8.0:
 - a. In the console, choose **Databases**, and then choose the read replica that you just created.
 - b. Choose **Modify**.
 - c. For **DB engine version**, choose the MySQL 8.0 version to upgrade to, and then choose **Continue**.
 - d. For **Scheduling of modifications**, choose **Apply immediately**.
 - e. Choose **Modify DB instance** to start the upgrade.
 5. When the upgrade is complete and **Status** shows **Available**, verify that the upgraded read replica is up-to-date with the source MySQL 5.7 DB instance. You can do this by connecting to the read replica and issuing the SHOW REPLICAS STATUS command. If the Seconds_Behind_Master field is 0, then replication is up-to-date.

Note

Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICAS STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

6. (Optional) Create a read replica of your read replica.

If you want the DB instance to have a read replica after it is promoted to a standalone DB instance, you can create the read replica now.

- a. In the console, choose **Databases**, and then choose the read replica that you just upgraded.
 - b. For **Actions**, choose **Create read replica**.
 - c. Provide a value for **DB instance identifier** for your read replica and ensure that the **DB instance class** and other settings match your MySQL 5.7 DB instance.
 - d. Choose **Create read replica**.
7. (Optional) Configure a custom DB parameter group for the read replica.
- If you want the DB instance to use a custom parameter group after it is promoted to a standalone DB instance, you can create the DB parameter group now and associate it with the read replica.
- a. Create a custom DB parameter group for MySQL 8.0. For instructions, see [Creating a DB parameter group \(p. 291\)](#).
 - b. Modify the parameters that you want to change in the DB parameter group you just created. For instructions, see [Modifying parameters in a DB parameter group \(p. 294\)](#).
 - c. In the console, choose **Databases**, and then choose the read replica.
 - d. Choose **Modify**.
 - e. For **DB parameter group**, choose the MySQL 8.0 DB parameter group you just created, and then choose **Continue**.
 - f. For **Scheduling of modifications**, choose **Apply immediately**.
 - g. Choose **Modify DB instance** to start the upgrade.
8. Make your MySQL 8.0 read replica a standalone DB instance.

Important

When you promote your MySQL 8.0 read replica to a standalone DB instance, it no longer is a replica of your MySQL 5.7 DB instance. We recommend that you promote your MySQL 8.0 read replica during a maintenance window when your source MySQL 5.7 DB instance is in read-only mode and all write operations are suspended. When the promotion is completed, you can direct your write operations to the upgraded MySQL 8.0 DB instance to ensure that no write operations are lost.

In addition, we recommend that, before promoting your MySQL 8.0 read replica, you perform all necessary data definition language (DDL) operations on your MySQL 8.0 read replica. An example is creating indexes. This approach avoids negative effects on the performance of the MySQL 8.0 read replica after it has been promoted. To promote a read replica, use the following procedure.

- a. In the console, choose **Databases**, and then choose the read replica that you just upgraded.
 - b. For **Actions**, choose **Promote**.
 - c. Choose **Yes** to enable automated backups for the read replica instance. For more information, see [Working with backups \(p. 427\)](#).
 - d. Choose **Continue**.
 - e. Choose **Promote Read Replica**.
9. You now have an upgraded version of your MySQL database. At this point, you can direct your applications to the new MySQL 8.0 DB instance.

Upgrading a MySQL DB snapshot

With Amazon RDS, you can create a storage volume DB snapshot of your MySQL DB instance. When you create a DB snapshot, the snapshot is based on the engine version used by your Amazon RDS instance. In addition to upgrading the DB engine version of your DB instance, you can also upgrade the engine version for your DB snapshots. For example, you can upgrade DB snapshots created from the MySQL 5.1 engine to DB snapshots for the MySQL 5.5 engine. After restoring a DB snapshot upgraded to a new engine version, you should test that the upgrade was successful. To learn how to test a major version upgrade, see [Testing an upgrade \(p. 1348\)](#). To learn how to restore a DB snapshot, see [Restoring from a DB snapshot \(p. 452\)](#).

Amazon RDS supports upgrading a MySQL DB snapshot from MySQL 5.1 to MySQL 5.5.

You can upgrade manual DB snapshots, which can be encrypted or not encrypted, from MySQL 5.1 to MySQL 5.5 within the same AWS Region. You can't upgrade automated DB snapshots that are created during the automated backup process.

Console

To upgrade a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. For **Actions**, choose **Upgrade snapshot**. The **Upgrade snapshot** page appears.
4. Choose the **New engine version** to upgrade to.
5. Choose **Save changes** to upgrade the snapshot.

During the upgrade process, all snapshot actions are disabled for this DB snapshot. Also, the DB snapshot status changes from **available** to **upgrading**, and then changes to **active** upon completion. If the DB snapshot can't be upgraded because of snapshot corruption issues, the status changes to **unavailable**. You can't recover the snapshot from this state.

Note

If the DB snapshot upgrade fails, the snapshot is rolled back to the original state with the original version.

AWS CLI

To upgrade a DB snapshot to a new database engine version, use the AWS CLI [modify-db-snapshot](#) command.

Parameters

- **--db-snapshot-identifier** – The identifier of the DB snapshot to upgrade. The identifier must be a unique Amazon Resource Name (ARN). For more information, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).
- **--engine-version** – The engine version to upgrade the DB snapshot to.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot \
```

```
--db-snapshot-identifier <mydbsnapshot> \
--engine-version <new_version>
```

For Windows:

```
aws rds modify-db-snapshot ^
--db-snapshot-identifier <mydbsnapshot> ^
--engine-version <new_version>
```

RDS API

To upgrade a DB snapshot to a new database engine version, call the Amazon RDS API [ModifyDBSnapshot](#) operation.

- **DBSnapshotIdentifier** – The identifier of the DB snapshot to upgrade. The identifier must be a unique Amazon Resource Name (ARN). For more information, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).
- **EngineVersion** – The engine version to upgrade the DB snapshot to.

Importing data into a MySQL DB instance

You can use several different techniques to import data into an RDS for MySQL DB instance. The best approach depends on the source of the data, the amount of data, and whether the import is done one time or is ongoing. If you are migrating an application along with the data, also consider the amount of downtime that you are willing to experience.

Overview

Find techniques to import data into an RDS for MySQL DB instance in the following table.

Source	Amount of data	One time or ongoing	Application downtime	Technique	More information
Existing MySQL database on premises or on Amazon EC2	Any	One time	Some	Create a backup of your on-premises database, store it on Amazon S3, and then restore the backup file to a new Amazon RDS DB instance running MySQL.	Restoring a backup into a MySQL DB instance (p. 1361)
Any existing database	Any	One time or ongoing	Minimal	Use AWS Database Migration Service to migrate the database with minimal downtime and, for many database DB engines, continue ongoing replication.	What is AWS Database Migration Service and Using a MySQL-compatible database as a target for AWS DMS in the AWS Database Migration Service User Guide
Existing MySQL DB instance	Any	One time or ongoing	Minimal	Create a read replica for ongoing replication. Promote the read replica for one-time creation of a new DB instance.	Working with read replicas (p. 370)
Existing MariaDB or MySQL database	Small	One time	Some	Copy the data directly to your MySQL DB instance using a command-line utility.	Importing data from a MariaDB or MySQL

Source	Amount of data	One time or ongoing	Application downtime	Technique	More information
					database to a MariaDB or MySQL DB instance (p. 1369)
Data not stored in an existing database	Medium	One time	Some	Create flat files and import them using the mysqlimport utility.	Importing data from any source to a MariaDB or MySQL DB instance (p. 1384)
Existing MariaDB or MySQL database on premises or on Amazon EC2	Any	Ongoing	Minimal	Configure replication with an existing MariaDB or MySQL database as the replication source.	Configuring binary log file position replication with an external source instance (p. 1408) Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime (p. 1371)

Note

The 'mysql' system database contains authentication and authorization information required to log in to your DB instance and access your data. Dropping, altering, renaming, or truncating tables, data, or other contents of the 'mysql' database in your DB instance can result in error and might render the DB instance and your data inaccessible. If this occurs, you can restore the DB instance from a snapshot using the AWS CLI `restore-db-instance-from-db-snapshot` command. You can recover the DB instance using the AWS CLI `restore-db-instance-to-point-in-time` command.

Importing data considerations

Following, you can find additional technical information related to loading data into MySQL. This information is intended for advanced users who are familiar with the MySQL server architecture. All comments related to LOAD DATA LOCAL INFILE also apply to mysqlimport.

Binary log

Data loads incur a performance penalty and require additional free disk space (up to four times more) when binary logging is enabled versus loading the same data with binary logging turned off. The severity of the performance penalty and the amount of free disk space required is directly proportional to the size of the transactions used to load the data.

Transaction size

Transaction size plays an important role in MySQL data loads. It has a major influence on resource consumption, disk space utilization, resume process, time to recover, and input format (flat files or SQL). This section describes how transaction size affects binary logging and makes the case for disabling binary logging during large data loads. As noted earlier, binary logging is enabled and disabled by setting the Amazon RDS automated backup retention period. Non-zero values enable binary logging, and zero disables it. We also describe the impact of large transactions on InnoDB and why it's important to keep transaction sizes small.

Small transactions

For small transactions, binary logging doubles the number of disk writes required to load the data. This effect can severely degrade performance for other database sessions and increase the time required to load the data. The degradation experienced depends in part upon the upload rate, other database activity taking place during the load, and the capacity of your Amazon RDS DB instance.

The binary logs also consume disk space roughly equal to the amount of data loaded until they are backed up and removed. Fortunately, Amazon RDS minimizes this by backing up and removing binary logs on a frequent basis.

Large transactions

Large transactions incur a 3X penalty for IOPS and disk consumption with binary logging enabled. This is due to the binary log cache spilling to disk, consuming disk space and incurring additional IO for each write. The cache cannot be written to the binlog until the transaction commits or rolls back, so it consumes disk space in proportion to the amount of data loaded. When the transaction commits, the cache must be copied to the binlog, creating a third copy of the data on disk.

Because of this, there must be at least three times as much free disk space available to load the data compared to loading with binary logging disabled. For example, 10 GiB of data loaded as a single transaction consumes at least 30 GiB disk space during the load. It consumes 10 GiB for the table + 10 GiB for the binary log cache + 10 GiB for the binary log itself. The cache file remains on disk until the session that created it terminates or the session fills its binary log cache again during another transaction. The binary log must remain on disk until backed up, so it might be some time before the extra 20 GiB is freed.

If the data was loaded using LOAD DATA LOCAL INFILE, yet another copy of the data is created if the database has to be recovered from a backup made before the load. During recovery, MySQL extracts the data from the binary log into a flat file. MySQL then runs LOAD DATA LOCAL INFILE, just as in the original transaction. However, this time the input file is local to the database server. Continuing with the example preceding, recovery fails unless there is at least 40 GiB free disk space available.

Disable binary logging

Whenever possible, disable binary logging during large data loads to avoid the resource overhead and addition disk space requirements. In Amazon RDS, disabling binary logging is as simple as setting the backup retention period to zero. If you do this, we recommend that you take a DB snapshot of the database instance immediately before the load. By doing this, you can quickly and easily undo changes made during loading if you need to.

After the load, set the backup retention period back to an appropriate (no zero) value.

You can't set the backup retention period to zero if the DB instance is a source DB instance for read replicas.

InnoDB

The information in this section provides a strong argument for keeping transaction sizes small when using InnoDB.

Undo

InnoDB generates undo to support features such as transaction rollback and MVCC. Undo is stored in the InnoDB system tablespace (usually `ibdata1`) and is retained until removed by the purge thread. The purge thread cannot advance beyond the undo of the oldest active transaction, so it is effectively blocked until the transaction commits or completes a rollback. If the database is processing other transactions during the load, their undo also accumulates in the system tablespace and cannot be removed even if they commit and no other transaction needs the undo for MVCC. In this situation, all transactions (including read-only transactions) that access any of the rows changed by any transaction (not just the load transaction) slow down. The slowdown occurs because transactions scan through undo that could have been purged if not for the long-running load transaction.

Undo is stored in the system tablespace, and the system tablespace never shrinks in size. Thus, large data load transactions can cause the system tablespace to become quite large, consuming disk space that you can't reclaim without recreating the database from scratch.

Rollback

InnoDB is optimized for commits. Rolling back a large transaction can take a very, very long time. In some cases, it might be faster to perform a point-in-time recovery or restore a DB snapshot.

Input data format

MySQL can accept incoming data in one of two forms: flat files and SQL. This section points out some key advantages and disadvantages of each.

Flat files

Loading flat files with `LOAD DATA LOCAL INFILE` can be the fastest and least costly method of loading data as long as transactions are kept relatively small. Compared to loading the same data with SQL, flat files usually require less network traffic, lowering transmission costs and load much faster due to the reduced overhead in the database.

One big transaction

`LOAD DATA LOCAL INFILE` loads the entire flat file as one transaction. This isn't necessarily a bad thing. If the size of the individual files can be kept small, this has a number of advantages:

- Resume capability – Keeping track of which files have been loaded is easy. If a problem arises during the load, you can pick up where you left off with little effort. Some data might have to be retransmitted to Amazon RDS, but with small files, the amount retransmitted is minimal.

- Load data in parallel – If you've got IOPS and network bandwidth to spare with a single file load, loading in parallel might save time.
- Throttle the load rate – Data load having a negative impact on other processes? Throttle the load by increasing the interval between files.

Be careful

The advantages of LOAD DATA LOCAL INFILE diminish rapidly as transaction size increases. If breaking up a large set of data into smaller ones isn't an option, SQL might be the better choice.

SQL

SQL has one main advantage over flat files: it's easy to keep transaction sizes small. However, SQL can take significantly longer to load than flat files and it can be difficult to determine where to resume the load after a failure. For example, mysqldump files are not restartable. If a failure occurs while loading a mysqldump file, the file requires modification or replacement before the load can resume. The alternative is to restore to the point in time before the load and replay the file after the cause of the failure has been corrected.

Take checkpoints using Amazon RDS snapshots

If you have a load that's going to take several hours or even days, loading without binary logging isn't a very attractive prospect unless you can take periodic checkpoints. This is where the Amazon RDS DB snapshot feature comes in very handy. A DB snapshot creates a point-in-time consistent copy of your database instance which can be used to restore the database to that point in time after a crash or other mishap.

To create a checkpoint, simply take a DB snapshot. Any previous DB snapshots taken for checkpoints can be removed without affecting durability or restore time.

Snapshots are fast too, so frequent checkpointing doesn't add significantly to load time.

Decreasing load time

Here are some additional tips to reduce load times:

- Create all secondary indexes before loading. This is counter-intuitive for those familiar with other databases. Adding or modifying a secondary index causes MySQL to create a new table with the index changes, copy the data from the existing table to the new table, and drop the original table.
- Load data in PK order. This is particularly helpful for InnoDB tables, where load times can be reduced by 75–80 percent and data file size cut in half.
- Disable foreign key constraints `foreign_key_checks=0`. For flat files loaded with LOAD DATA LOCAL INFILE, this is required in many cases. For any load, disabling FK checks provides significant performance gains. Just be sure to enable the constraints and verify the data after the load.
- Load in parallel unless already near a resource limit. Use partitioned tables when appropriate.
- Use multi-value inserts when loading with SQL to minimize overhead when running statements. When using mysqldump, this is done automatically.
- Reduce InnoDB log IO `innodb_flush_log_at_trx_commit=0`
- If you are loading data into a DB instance that does not have read replicas, set the `sync_binlog` parameter to 0 while loading data. When data loading is complete, set the `sync_binlog` parameter back to 1.
- Load data before converting the DB instance to a Multi-AZ deployment. However, if the DB instance already uses a Multi-AZ deployment, switching to a Single-AZ deployment for data loading is not recommended, because doing so only provides marginal improvements.

Note

Using `innodb_flush_log_at_trx_commit=0` causes InnoDB to flush its logs every second instead of at each commit. This provides a significant speed advantage, but can lead to data loss during a crash. Use with caution.

Topics

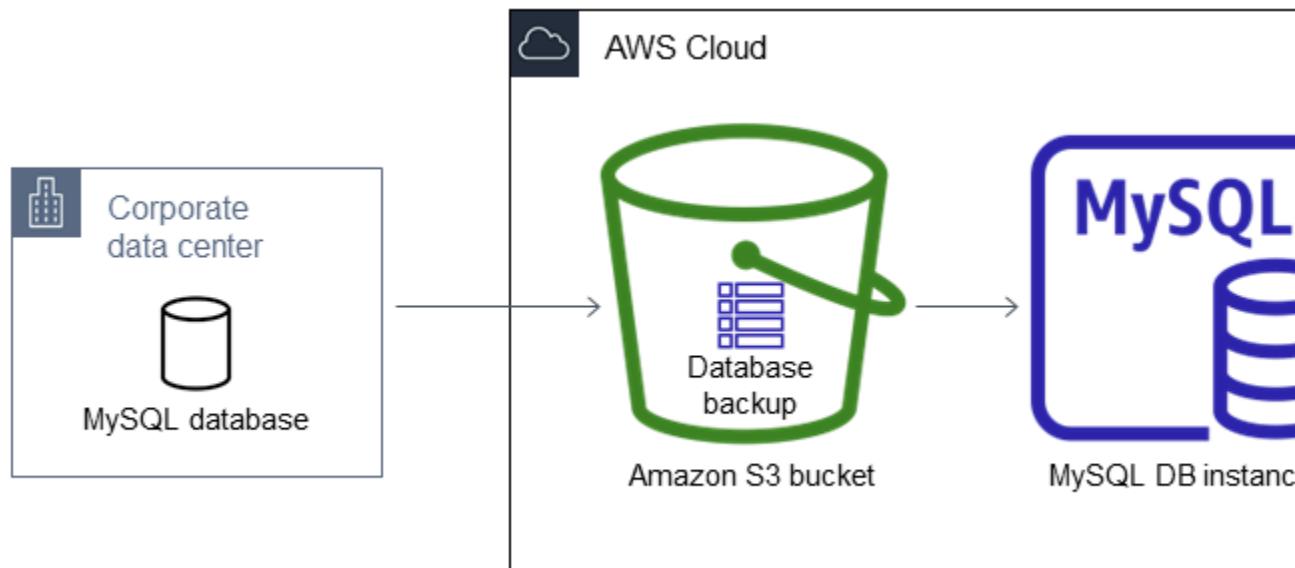
- [Restoring a backup into a MySQL DB instance \(p. 1361\)](#)
- [Importing data from a MariaDB or MySQL database to a MariaDB or MySQL DB instance \(p. 1369\)](#)
- [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#)
- [Importing data from any source to a MariaDB or MySQL DB instance \(p. 1384\)](#)

Restoring a backup into a MySQL DB instance

Amazon RDS supports importing MySQL databases by using backup files. You can create a backup of your database, store it on Amazon S3, and then restore the backup file onto a new Amazon RDS DB instance running MySQL.

The scenario described in this section restores a backup of an on-premises database. You can use this technique for databases in other locations, such as Amazon EC2 or non-AWS cloud services, as long as the database is accessible.

You can find the supported scenario in the following diagram.



Importing backup files from Amazon S3 is supported for MySQL in all AWS Regions.

We recommend that you import your database to Amazon RDS by using backup files if your on-premises database can be offline while the backup file is created, copied, and restored. If your database can't be offline, you can use binary log (binlog) replication to update your database after you have migrated to Amazon RDS through Amazon S3 as explained in this topic. For more information, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#). You can also use the AWS Database Migration Service to migrate your database to Amazon RDS. For more information, see [What is AWS Database Migration Service?](#)

Limitations and recommendations for importing backup files from Amazon S3 to Amazon RDS

The following are some limitations and recommendations for importing backup files from Amazon S3:

- You can only import your data to a new DB instance, not an existing DB instance.
- You must use Percona XtraBackup to create the backup of your on-premises database.
- You can't import data from a DB snapshot export to Amazon S3.
- You can't migrate from a source database that has tables defined outside of the default MySQL data directory.
- You must import your data to the default minor version of your MySQL major version in your AWS Region. For example, if your major version is MySQL 8.0, and the default minor version for your AWS Region is 8.0.28, then you must import your data into a MySQL version 8.0.28 DB instance. You can

upgrade your DB instance after importing. For information about determining the default minor version, see [MySQL on Amazon RDS versions \(p. 1315\)](#).

- Backward migration is not supported for both major versions and minor versions. For example, you can't migrate from version 8.0 to version 5.7, and you can't migrate from version 8.0.28 to version 8.0.27.
- You can't import a MySQL 5.5 or 5.6 database.
- You can't import an on-premises MySQL database from one major version to another. For example, you can't import a MySQL 5.7 database to an RDS for MySQL 8.0 database. You can upgrade your DB instance after you complete the import.
- You can't restore from an encrypted source database, but you can restore to an encrypted Amazon RDS DB instance.
- You can't restore from an encrypted backup in the Amazon S3 bucket.
- You can't restore from an Amazon S3 bucket in a different AWS Region than your Amazon RDS DB instance.
- Importing from Amazon S3 is not supported on the db.t2.micro DB instance class. However, you can restore to a different DB instance class, and change the DB instance class later. For more information about instance classes, see [Hardware specifications for DB instance classes \(p. 55\)](#).
- Amazon S3 limits the size of a file uploaded to an Amazon S3 bucket to 5 TB. If a backup file exceeds 5 TB, then you must split the backup file into smaller files.
- When you restore the database, the backup is copied and then extracted on your DB instance. Therefore, provision storage space for your DB instance that is equal to or greater than the sum of the backup size, plus the original database's size on disk.
- Amazon RDS limits the number of files uploaded to an Amazon S3 bucket to 1 million. If the backup data for your database, including all full and incremental backups, exceeds 1 million files, use a Gzip (.gz), tar (.tar.gz), or Percona xbstream (.xbstream) file to store full and incremental backup files in the Amazon S3 bucket. Percona XtraBackup 8.0 only supports Percona xbstream for compression.
- User accounts are not imported automatically. Save your user accounts from your source database and add them to your new DB instance later.
- Functions are not imported automatically. Save your functions from your source database and add them to your new DB instance later.
- Stored procedures are not imported automatically. Save your stored procedures from your source database and add them to your new DB instance later.
- Time zone information is not imported automatically. Record the time zone information for your source database, and set the time zone of your new DB instance later. For more information, see [Local time zone for MySQL DB instances \(p. 1433\)](#).
- The `innodb_data_file_path` parameter must be configured with only one data file that uses the default data file name "ibdata1:12M:autoextend". Databases with two data files, or with a data file with a different name, can't be migrated using this method.

The following are examples of file names that are not allowed:

"`innodb_data_file_path=ibdata1:50M; ibdata2:50M:autoextend`" and
"`innodb_data_file_path=ibdata01:50M:autoextend`".

- The maximum size of the restored database is the maximum database size supported minus the size of the backup. So, if the maximum database size supported is 64 TiB, and the size of the backup is 30 TiB, then the maximum size of the restored database is 34 TiB, as in the following example:

$$64 \text{ TiB} - 30 \text{ TiB} = 34 \text{ TiB}$$

For information about the maximum database size supported by Amazon RDS for MySQL, see [General Purpose SSD storage \(p. 64\)](#) and [Provisioned IOPS SSD storage \(p. 66\)](#).

Overview of setting up to import backup files from Amazon S3 to Amazon RDS

These are the components you need to set up to import backup files from Amazon S3 to Amazon RDS:

- An Amazon S3 bucket to store your backup files.
- A backup of your on-premises database created by Percona XtraBackup.
- An AWS Identity and Access Management (IAM) role to allow Amazon RDS to access the bucket.

If you already have an Amazon S3 bucket, you can use that. If you don't have an Amazon S3 bucket, you can create a new one. If you want to create a new bucket, see [Creating a bucket](#).

Use the Percona XtraBackup tool to create your backup. For more information, see [Creating your database backup \(p. 1363\)](#).

If you already have an IAM role, you can use that. If you don't have an IAM role, you can create a new one manually. Alternatively, you can choose to have a new IAM role created for you in your account by the wizard when you restore the database by using the AWS Management Console. If you want to create a new IAM role manually, or attach trust and permissions policies to an existing IAM role, see [Creating an IAM role manually \(p. 1365\)](#). If you want to have a new IAM role created for you, follow the procedure in [Console \(p. 1366\)](#).

Creating your database backup

Use the Percona XtraBackup software to create your backup. You can install Percona XtraBackup from [Download Percona XtraBackup](#).

Warning

When creating a database backup, XtraBackup might save credentials in the `xtrabackup_info` file. Make sure you examine that file so that the `tool_command` setting in it doesn't contain any sensitive information.

Note

For MySQL 8.0 migration, you must use Percona XtraBackup 8.0. Percona XtraBackup 8.0.12 and higher versions support migration of all versions of MySQL. If you are migrating to RDS for MySQL 8.0.20 or higher, you must use Percona XtraBackup 8.0.12 or higher.

For MySQL 5.7 migrations, you can also use Percona XtraBackup 2.4. For migrations of earlier MySQL versions, you can also use Percona XtraBackup 2.3 or 2.4.

You can create a full backup of your MySQL database files using Percona XtraBackup. Alternatively, if you already use Percona XtraBackup to back up your MySQL database files, you can upload your existing full and incremental backup directories and files.

For more information about backing up your database with Percona XtraBackup, see [Percona XtraBackup - documentation](#) and [The xtrabackup binary](#) on the Percona website.

Creating a full backup with Percona XtraBackup

To create a full backup of your MySQL database files that can be restored from Amazon S3, use the Percona XtraBackup utility (`xtrabackup`) to back up your database.

For example, the following command creates a backup of a MySQL database and stores the files in the folder `/on-premises/s3-restore/backup` folder.

```
xtrabackup --backup --user=<myuser> --password=<password> --target-dir=</on-premises/s3-restore/backup>
```

If you want to compress your backup into a single file (which can be split later, if needed), you can save your backup in one of the following formats:

- Gzip (.gz)
- tar (.tar)
- Percona xbstream (.xbstream)

Note

Percona XtraBackup 8.0 only supports Percona xbstream for compression.

The following command creates a backup of your MySQL database split into multiple Gzip files.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \  
--target-dir=</on-premises/s3-restore/backup> | gzip - | split -d --bytes=500MB \  
- </on-premises/s3-restore/backup/backup>.tar.gz
```

The following command creates a backup of your MySQL database split into multiple tar files.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \  
--target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \  
- </on-premises/s3-restore/backup/backup>.tar
```

The following command creates a backup of your MySQL database split into multiple xbstream files.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=xbstream \  
--target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \  
- </on-premises/s3-restore/backup/backup>.xbstream
```

Using incremental backups with Percona XtraBackup

If you already use Percona XtraBackup to perform full and incremental backups of your MySQL database files, you don't need to create a full backup and upload the backup files to Amazon S3. Instead, you can save a significant amount of time by copying your existing backup directories and files to your Amazon S3 bucket. For more information about creating incremental backups using Percona XtraBackup, see [Incremental backup](#).

When copying your existing full and incremental backup files to an Amazon S3 bucket, you must recursively copy the contents of the base directory. Those contents include the full backup and also all incremental backup directories and files. This copy must preserve the directory structure in the Amazon S3 bucket. Amazon RDS iterates through all files and directories. Amazon RDS uses the `xtrabackup-checkpoints` file that is included with each incremental backup to identify the base directory, and to order incremental backups by log sequence number (LSN) range.

Backup considerations for Percona XtraBackup

Amazon RDS consumes your backup files based on the file name. Name your backup files with the appropriate file extension based on the file format—for example, .xbstream for files stored using the Percona xbstream format.

Amazon RDS consumes your backup files in alphabetical order and also in natural number order. Use the `split` option when you issue the `xtrabackup` command to ensure that your backup files are written and named in the proper order.

Amazon RDS doesn't support partial backups created using Percona XtraBackup. You can't use the following options to create a partial backup when you back up the source files for your database: --

tables, --tables-exclude, --tables-file, --databases, --databases-exclude, or --databases-file.

Amazon RDS supports incremental backups created using Percona XtraBackup. For more information about creating incremental backups using Percona XtraBackup, see [Incremental backup](#).

Creating an IAM role manually

If you don't have an IAM role, you can create a new one manually. Alternatively, you can choose to have a new IAM role created for you by the wizard when you restore the database by using the AWS Management Console. If you want to have a new IAM role created for you, follow the procedure in [Console \(p. 1366\)](#).

To manually create a new IAM role for importing your database from Amazon S3, create a role to delegate permissions from Amazon RDS to your Amazon S3 bucket. When you create an IAM role, you attach trust and permissions policies. To import your backup files from Amazon S3, use trust and permissions policies similar to the examples following. For more information about creating the role, see [Creating a role to delegate permissions to an AWS service](#).

Alternatively, you can choose to have a new IAM role created for you by the wizard when you restore the database by using the AWS Management Console. If you want to have a new IAM role created for you, follow the procedure in [Console \(p. 1366\)](#)

The trust and permissions policies require that you provide an Amazon Resource Name (ARN). For more information about ARN formatting, see [Amazon Resource Names \(ARNs\) and AWS service namespaces](#).

Example Trust policy for importing from Amazon S3

```
{  
    "Version": "2012-10-17",  
    "Statement":  
    [ {  
        "Effect": "Allow",  
        "Principal": {"Service": "rds.amazonaws.com"},  
        "Action": "sts:AssumeRole"  
    } ]  
}
```

Example Permissions policy for importing from Amazon S3 — IAM user permissions

```
{  
    "Version": "2012-10-17",  
    "Statement":  
    [ {  
        "Sid": "AllowS3AccessRole",  
        "Effect": "Allow",  
        "Action": "iam:PassRole",  
        "Resource": "arn:aws:iam::IAM User ID:role/S3Access"  
    } ]  
}
```

Example Permissions policy for importing from Amazon S3 — role permissions

```
{  
    "Version": "2012-10-17",  
}
```

```
"Statement":  
[  
    {  
        "Effect": "Allow",  
        "Action":  
            [  
                "s3>ListBucket",  
                "s3:GetBucketLocation"  
            ],  
        "Resource": "arn:aws:s3:::bucket_name"  
    },  
    {  
        "Effect": "Allow",  
        "Action":  
            [  
                "s3GetObject"  
            ],  
        "Resource": "arn:aws:s3:::bucket_name/prefix*"  
    }  
]
```

Note

If you include a file name prefix, include the asterisk (*) after the prefix. If you don't want to specify a prefix, specify only an asterisk.

Importing data from Amazon S3 to a new MySQL DB instance

You can import data from Amazon S3 to a new MySQL DB instance using the AWS Management Console, AWS CLI, or RDS API.

Console

To import data from Amazon S3 to a new MySQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top right corner of the Amazon RDS console, choose the AWS Region in which to create your DB instance. Choose the same AWS Region as the Amazon S3 bucket that contains your database backup.
3. In the navigation pane, choose **Databases**.
4. Choose **Restore from S3**.

The **Create database by restoring from S3** page appears.

RDS > Create database

Create database by restoring from S3

S3 destination



Write audit logs to S3

Enter a destination in Amazon S3 where your audit logs will be stored. Amazon S3 is object storage build to store and retrieve any amount of data from anywhere

S3 bucket

test-eu1-bucket



S3 prefix (optional) [Info](#)

Engine options

Engine type [Info](#)



Amazon Aurora



MySQL



Edition

MySQL Community

Source engine version [Info](#)

5.6



Version [Info](#)

MySQL 5.6.44



Known Issues/Limitations

Review the [Known Issues/Limitations](#) to learn about potential compatibility issues with specific database versions.

IAM role



IAM role

Choose or create an IAM role to grant write access to your S3 bucket.

[Choose an option](#)



Settings

1367

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

5. Under **S3 destination**:

- a. Choose the **S3 bucket** where to write audit logs.
- b. (Optional) For **S3 folder path prefix**, enter a file path prefix for the files stored in your Amazon S3 bucket.

If you don't specify a prefix, then RDS creates your DB instance using all of the files and folders in the root folder of the S3 bucket. If you do specify a prefix, then RDS creates your DB instance using the files and folders in the S3 bucket where the path for the file begins with the specified prefix.

For example, suppose that you store your backup files on S3 in a subfolder named backups, and you have multiple sets of backup files, each in its own directory (gzip_backup1, gzip_backup2, and so on). In this case, you specify a prefix of backups/gzip_backup1 to restore from the files in the gzip_backup1 folder.

6. Under **Engine options**:

- a. For **Engine type**, choose **MySQL**.
- b. For **Source engine version**, choose the MySQL major version of your source database.
- c. For **Version**, choose the default minor version of your MySQL major version in your AWS Region.

In the AWS Management Console, only the default minor version is available. You can upgrade your DB instance after importing.

7. For **IAM role**, you can choose an existing IAM role.
8. (Optional) You can also have a new IAM role created for you by choosing **Create a new role** and entering the **IAM role name**.
9. Specify your DB instance information. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Note

Be sure to allocate enough memory for your new DB instance so that the restore operation can succeed.

You can also choose **Enable storage autoscaling** to allow for future growth automatically.

10. Choose additional settings as needed.

11. Choose **Create database**.

AWS CLI

To import data from Amazon S3 to a new MySQL DB instance by using the AWS CLI, call the `restore-db-instance-from-s3` command with the following parameters. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Note

Be sure to allocate enough memory for your new DB instance so that the restore operation can succeed.

You can also use the `--max-allocated-storage` parameter to enable storage autoscaling and allow for future growth automatically.

- `--allocated-storage`
- `--db-instance-identifier`
- `--db-instance-class`
- `--engine`
- `--master-username`
- `--master-user-password`
- `--s3-bucket-name`

- `--s3-ingestion-role-arn`
- `--s3-prefix`
- `--source-engine`
- `--source-engine-version`

Example

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-from-s3 \
  --allocated-storage 250 \
  --db-instance-identifier myidentifier \
  --db-instance-class db.m5.large \
  --engine mysql \
  --master-username admin \
  --master-user-password mypassword \
  --s3-bucket-name mybucket \
  --s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename \
  --s3-prefix bucketprefix \
  --source-engine mysql \
  --source-engine-version 8.0.28 \
  --max-allocated-storage 1000
```

For Windows:

```
aws rds restore-db-instance-from-s3 ^
  --allocated-storage 250 ^
  --db-instance-identifier myidentifier ^
  --db-instance-class db.m5.large ^
  --engine mysql ^
  --master-username admin ^
  --master-user-password mypassword ^
  --s3-bucket-name mybucket ^
  --s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename ^
  --s3-prefix bucketprefix ^
  --source-engine mysql ^
  --source-engine-version 8.0.28 ^
  --max-allocated-storage 1000
```

RDS API

To import data from Amazon S3 to a new MySQL DB instance by using the Amazon RDS API, call the [RestoreDBInstanceFromS3](#) operation.

Importing data from a MariaDB or MySQL database to a MariaDB or MySQL DB instance

You can also import data from an existing MariaDB or MySQL database to a MySQL or MariaDB DB instance. You do so by copying the database with [mysqldump](#) and piping it directly into the MariaDB or MySQL DB instance. The mysqldump command line utility is commonly used to make backups and transfer data from one MariaDB or MySQL server to another. It's included with MySQL and MariaDB client software.

Note

If you are using a MySQL DB instance and your scenario supports it, it's easier to move data in and out of Amazon RDS by using backup files and Amazon S3. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

A typical mysqldump command to move data from an external database to an Amazon RDS DB instance looks similar to the following.

```
mysqldump -u local_user \  
  --databases database_name \  
  --single-transaction \  
  --compress \  
  --order-by-primary \  
  -plocal_password | mysql -u RDS_user \  
    --port=port_number \  
    --host=host_name \  
    -pRDS_password
```

Important

Make sure not to leave a space between the `-p` option and the entered password.

Make sure that you're aware of the following recommendations and considerations:

- Exclude the following schemas from the dump file: `sys`, `performance_schema`, and `information_schema`. The `mysqldump` utility excludes these schemas by default.
- If you need to migrate users and privileges, consider using a tool that generates the data control language (DCL) for recreating them, such as the [pt-show-grants](#) utility.
- To perform the import, make sure the user doing so has access to the DB instance. For more information, see [Controlling access with security groups \(p. 2085\)](#).

The parameters used are as follows:

- `-u local_user` – Use to specify a user name. In the first usage of this parameter, you specify the name of a user account on the local MariaDB or MySQL database identified by the `--databases` parameter.
- `--databases database_name` – Use to specify the name of the database on the local MariaDB or MySQL instance that you want to import into Amazon RDS.
- `--single-transaction` – Use to ensure that all of the data loaded from the local database is consistent with a single point in time. If there are other processes changing the data while `mysqldump` is reading it, using this parameter helps maintain data integrity.
- `--compress` – Use to reduce network bandwidth consumption by compressing the data from the local database before sending it to Amazon RDS.
- `--order-by-primary` – Use to reduce load time by sorting each table's data by its primary key.
- `-plocal_password` – Use to specify a password. In the first usage of this parameter, you specify the password for the user account identified by the first `-u` parameter.
- `-u RDS_user` – Use to specify a user name. In the second usage of this parameter, you specify the name of a user account on the default database for the MariaDB or MySQL DB instance identified by the `--host` parameter.
- `--port port_number` – Use to specify the port for your MariaDB or MySQL DB instance. By default, this is 3306 unless you changed the value when creating the instance.
- `--host host_name` – Use to specify the Domain Name System (DNS) name from the Amazon RDS DB instance endpoint, for example, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. You can find the endpoint value in the instance details in the Amazon RDS Management Console.
- `-pRDS_password` – Use to specify a password. In the second usage of this parameter, you specify the password for the user account identified by the second `-u` parameter.

Make sure to create any stored procedures, triggers, functions, or events manually in your Amazon RDS database. If you have any of these objects in the database that you are copying, then exclude them when

you run `mysqldump`. To do so, include the following parameters with your `mysqldump` command: `--routines=0 --triggers=0 --events=0`.

The following example copies the `world` sample database on the local host to a MySQL DB instance.

For Linux, macOS, or Unix:

```
sudo mysqldump -u localuser \  
  --databases world \  
  --single-transaction \  
  --compress \  
  --order-by-primary \  
  --routines=0 \  
  --triggers=0 \  
  --events=0 \  
  -plocalpassword | mysql -u rdsuser \  
    --port=3306 \  
    --host=myinstance.123456789012.us-east-1.rds.amazonaws.com \  
    -prdspassword
```

For Windows, run the following command in a command prompt that has been opened by right-clicking **Command Prompt** on the Windows programs menu and choosing **Run as administrator**:

```
mysqldump -u localuser ^  
  --databases world ^  
  --single-transaction ^  
  --compress ^  
  --order-by-primary ^  
  --routines=0 ^  
  --triggers=0 ^  
  --events=0 ^  
  -plocalpassword | mysql -u rdsuser ^  
    --port=3306 ^  
    --host=myinstance.123456789012.us-east-1.rds.amazonaws.com ^  
    -prdspassword
```

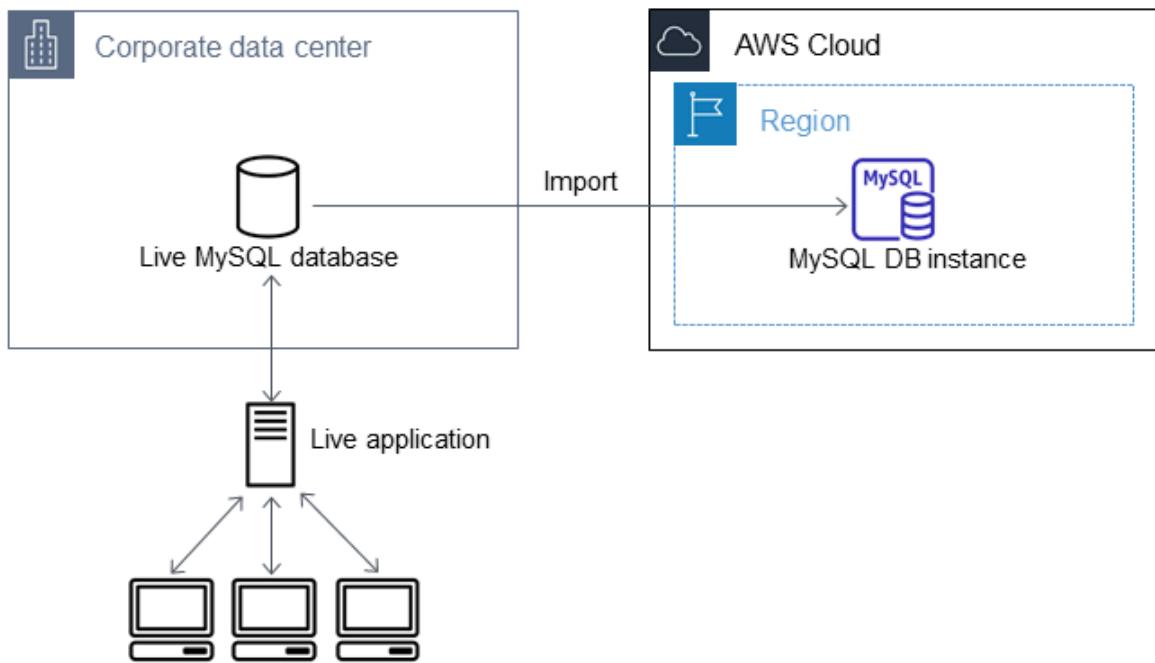
Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime

In some cases, you might need to import data from an external MariaDB or MySQL database that supports a live application to a MariaDB or MySQL DB instance. In these cases, you can use the following procedure to minimize the impact on application availability. This procedure can also help if you are working with a very large database. Here, the procedure helps because you can reduce the cost of the import by reducing the amount of data that is passed across the network to AWS.

In this procedure, you transfer a copy of your database data to an Amazon EC2 instance and import the data into a new Amazon RDS DB instance. You then use replication to bring the Amazon RDS DB instance up-to-date with your live external instance, before redirecting your application to the Amazon RDS DB instance. You configure MariaDB replication based on global transaction identifiers (GTIDs) if the external instance is MariaDB 10.0.24 or higher and the target instance is RDS for MariaDB. Otherwise, you configure replication based on binary log coordinates. We recommend GTID-based replication if your external database supports it due to its enhanced crash-safety features. For more information, see [Global transaction ID](#) in the MariaDB documentation.

Note

If you want to import data into a MySQL DB instance and your scenario supports it, it is easier to move data in and out of Amazon RDS by using backup files and Amazon S3. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

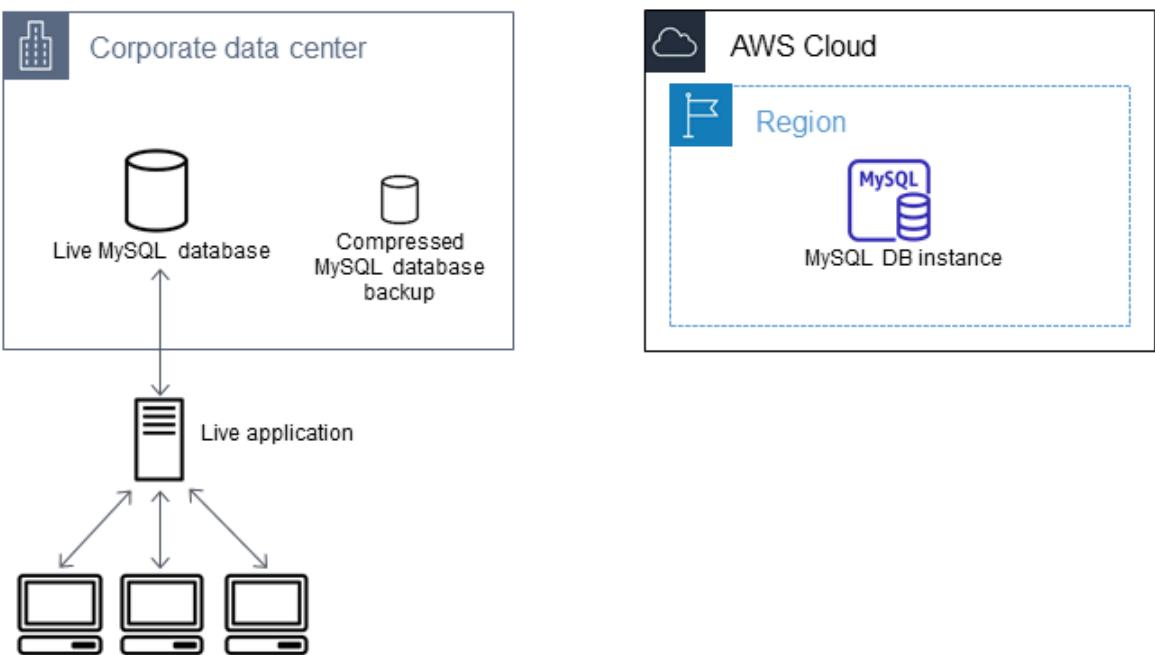


Note

We don't recommend that you use this procedure with source MySQL databases from MySQL versions earlier than version 5.5, due to potential replication issues. For more information, see [Replication compatibility between MySQL versions](#) in the MySQL documentation.

Create a copy of your existing database

The first step in the process of migrating a large amount of data to an Amazon RDS MariaDB or MySQL DB instance with minimal downtime is to create a copy of the source data.



You can use the mysqldump utility to create a database backup in either SQL or delimited-text format. We recommend that you do a test run with each format in a nonproduction environment to see which method minimizes the amount of time that mysqldump runs.

We also recommend that you weigh mysqldump performance against the benefit offered by using the delimited-text format for loading. A backup using delimited-text format creates a tab-separated text file for each table being dumped. To reduce the amount of time required to import your database, you can load these files in parallel using the `LOAD DATA LOCAL INFILE` command. For more information about choosing a mysqldump format and then loading the data, see [Using mysqldump for backups](#) in the MySQL documentation.

Before you start the backup operation, make sure to set the replication options on the MariaDB or MySQL database that you are copying to Amazon RDS. The replication options include turning on binary logging and setting a unique server ID. Setting these options causes your server to start logging database transactions and prepares it to be a source replication instance later in this process.

Note

Use the `--single-transaction` option with mysqldump because it dumps a consistent state of the database. To ensure a valid dump file, don't run data definition language (DDL) statements while mysqldump is running. You can schedule a maintenance window for these operations.

Exclude the following schemas from the dump file: `sys`, `performance_schema`, and `information_schema`. The mysqldump utility excludes these schemas by default.

To migrate users and privileges, consider using a tool that generates the data control language (DCL) for recreating them, such as the [pt-show-grants](#) utility.

To set replication options

1. Edit the `my.cnf` file (this file is usually under `/etc`).

```
sudo vi /etc/my.cnf
```

Add the `log_bin` and `server_id` options to the `[mysqld]` section. The `log_bin` option provides a file name identifier for binary log files. The `server_id` option provides a unique identifier for the server in source-replica relationships.

The following example shows the updated `[mysqld]` section of a `my.cnf` file.

```
[mysqld]
log-bin=mysql-bin
server-id=1
```

For more information, see [the MySQL documentation](#).

2. Restart the `mysql` service.

```
sudo service mysqld restart
```

To create a backup copy of your existing database

1. Create a backup of your data using the mysqldump utility, specifying either SQL or delimited-text format.

Specify `--master-data=2` to create a backup file that can be used to start replication between servers. For more information, see the [mysqldump](#) documentation.

To improve performance and ensure data integrity, use the `--order-by-primary` and `--single-transaction` options of `mysqldump`.

To avoid including the MySQL system database in the backup, do not use the `--all-databases` option with `mysqldump`. For more information, see [Creating a data snapshot using mysqldump](#) in the MySQL documentation.

Use `chmod` if necessary to make sure that the directory where the backup file is being created is writeable.

Important

On Windows, run the command window as an administrator.

- To produce SQL output, use the following command.

For Linux, macOS, or Unix:

```
sudo mysqldump \  
    --databases database_name \  
    --master-data=2 \  
    --single-transaction \  
    --order-by-primary \  
    -r backup.sql \  
    -u local_user \  
    -p password
```

For Windows:

```
mysqldump ^  
    --databases database_name ^  
    --master-data=2 ^  
    --single-transaction ^  
    --order-by-primary ^  
    -r backup.sql ^  
    -u local_user ^  
    -p password
```

- To produce delimited-text output, use the following command.

For Linux, macOS, or Unix:

```
sudo mysqldump \  
    --tab=target_directory \  
    --fields-terminated-by ',' ' \  
    --fields-enclosed-by '\"' \  
    --lines-terminated-by 0x0d0a \  
    database_name \  
    --master-data=2 \  
    --single-transaction \  
    --order-by-primary \  
    -p password
```

For Windows:

```
mysqldump ^  
    --tab=target_directory ^  
    --fields-terminated-by "," ^  
    --fields-enclosed-by "\"" ^  
    --lines-terminated-by 0x0d0a ^  
    database_name ^
```

```
--master-data=2 ^  
--single-transaction ^  
--order-by-primary ^  
-p password
```

Note

Make sure to create any stored procedures, triggers, functions, or events manually in your Amazon RDS database. If you have any of these objects in the database that you are copying, exclude them when you run mysqldump. To do so, include the following arguments with your mysqldump command: `--routines=0 --triggers=0 --events=0`.

When using the delimited-text format, a CHANGE MASTER TO comment is returned when you run mysqldump. This comment contains the master log file name and position. If the external instance is other than MariaDB version 10.0.24 or higher, note the values for `MASTER_LOG_FILE` and `MASTER_LOG_POS`. You need these values when setting up replication.

```
-- Position to start replication or point-in-time recovery from  
--  
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

If you are using SQL format, you can get the master log file name and position in the CHANGE MASTER TO comment in the backup file. If the external instance is MariaDB version 10.0.24 or higher, you can get the GTID in the next step.

2. If the external instance you are using is MariaDB version 10.0.24 or higher, you use GTID-based replication. Run `SHOW MASTER STATUS` on the external MariaDB instance to get the binary log file name and position, then convert them to a GTID by running `BINLOG_GTID_POS` on the external MariaDB instance.

```
SELECT BINLOG_GTID_POS('binary log file name', binary log file position);
```

Note the GTID returned; you need it to configure replication.

3. Compress the copied data to reduce the amount of network resources needed to copy your data to the Amazon RDS DB instance. Take note of the size of the backup file; you need this information when determining how large an Amazon EC2 instance to create. When you are done, compress the backup file using GZIP or your preferred compression utility.

- To compress SQL output, use the following command.

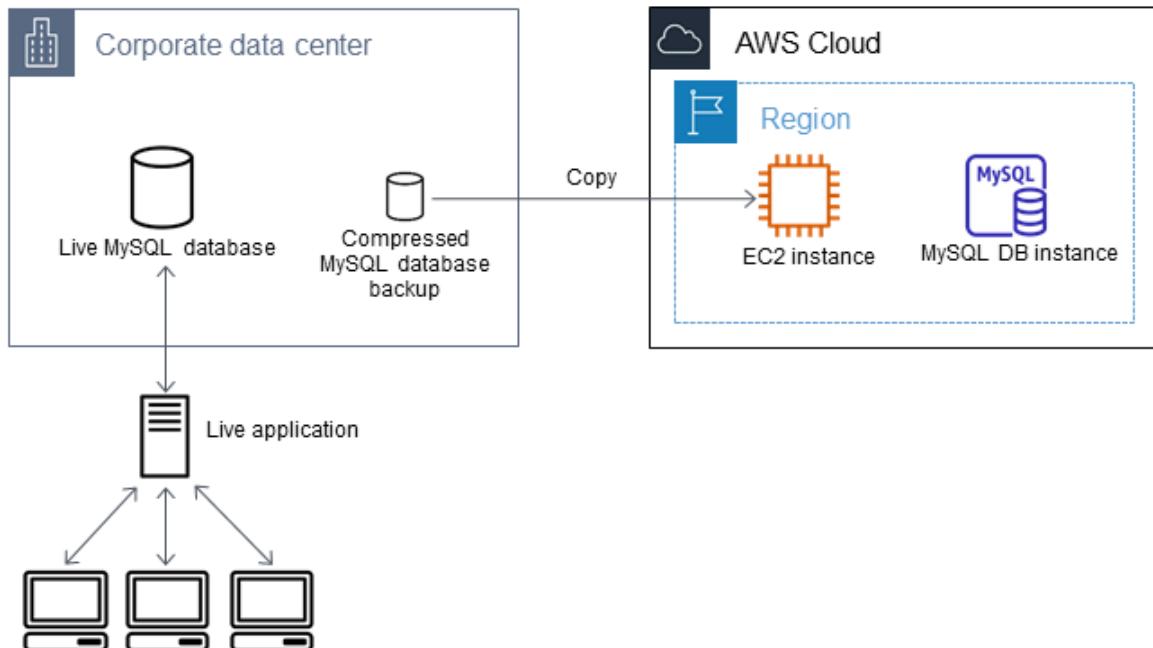
```
gzip backup.sql
```

- To compress delimited-text output, use the following command.

```
tar -zcvf backup.tar.gz target_directory
```

Create an Amazon EC2 instance and copy the compressed database

Copying your compressed database backup file to an Amazon EC2 instance takes fewer network resources than doing a direct copy of uncompressed data between database instances. After your data is in Amazon EC2, you can copy it from there directly to your MariaDB or MySQL DB instance. For you to save on the cost of network resources, your Amazon EC2 instance must be in the same AWS Region as your Amazon RDS DB instance. Having the Amazon EC2 instance in the same AWS Region as your Amazon RDS DB instance also reduces network latency during the import.



To create an Amazon EC2 instance and copy your data

1. In the AWS Region where you plan to create the RDS DB instance to run your MySQL database engine, create a virtual private cloud (VPC), a VPC security group, and a VPC subnet. Ensure that the inbound rules for your VPC security group allow the IP addresses required for your application to connect to AWS. This can be a range of IP addresses (for example, 203 . 0 . 113 . 0/24), or another VPC security group. You can use the [Amazon VPC Management Console](#) to create and manage VPCs, subnets, and security groups. For more information, see [Getting started with Amazon VPC](#) in the *Amazon Virtual Private Cloud Getting Started Guide*.
2. Open the [Amazon EC2 Management Console](#) and choose the AWS Region to contain both your Amazon EC2 instance and your Amazon RDS DB instance. Launch an Amazon EC2 instance using the VPC, subnet, and security group that you created in Step 1. Ensure that you select an instance type with enough storage for your database backup file when it is uncompressed. For details on Amazon EC2 instances, see [Getting started with Amazon EC2 Linux instances](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.
3. To connect to your Amazon RDS DB instance from your Amazon EC2 instance, edit your VPC security group. Add an inbound rule specifying the private IP address of your EC2 instance. You can find the private IP address on the **Details** tab of the **Instance** pane in the EC2 console window. To edit the VPC security group and add an inbound rule, choose **Security Groups** in the EC2 console navigation pane, choose your security group, and then add an inbound rule for MySQL or Aurora specifying the private IP address of your EC2 instance. To learn how to add an inbound rule to a VPC security group, see [Adding and removing rules](#) in the *Amazon VPC User Guide*.
4. Copy your compressed database backup file from your local system to your Amazon EC2 instance. Use chmod if necessary to make sure that you have write permission for the target directory of the Amazon EC2 instance. You can use scp or a Secure Shell (SSH) client to copy the file. The following is an example.

```
$ scp -r -i key_pair.pem backup.sql.gz ec2-user@EC2 DNS:/target_directory/backup.sql.gz
```

Important

Be sure to copy sensitive data using a secure network transfer protocol.

5. Connect to your Amazon EC2 instance and install the latest updates and the MySQL client tools using the following commands.

```
sudo yum update -y  
sudo yum install mysql -y
```

For more information, see [Connect to your instance](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.

Important

This example installs the MySQL client on an Amazon Machine Image (AMI) for an Amazon Linux distribution. To install the MySQL client on a different distribution, such as Ubuntu or RedHat Enterprise Linux, this example doesn't work. For information about installing MySQL, see [Installing and Upgrading MySQL](#) in the MySQL documentation.

6. While connected to your Amazon EC2 instance, decompress your database backup file. The following are examples.

- To decompress SQL output, use the following command.

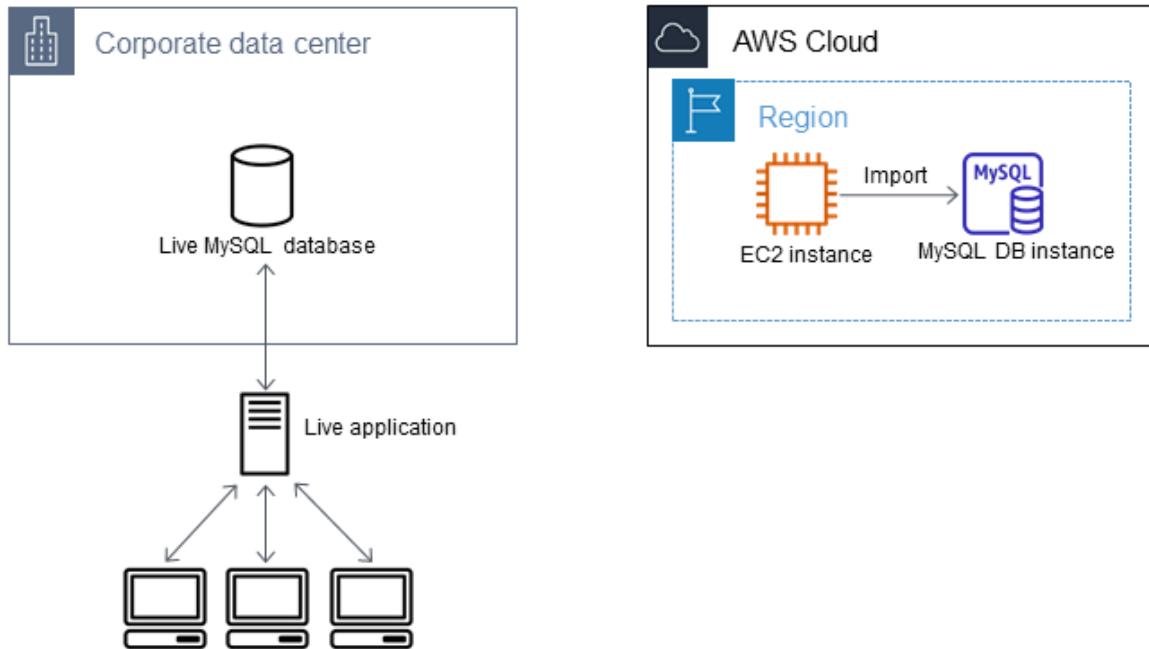
```
gzip backup.sql.gz -d
```

- To decompress delimited-text output, use the following command.

```
tar xzvf backup.tar.gz
```

Create a MySQL or MariaDB DB instance and import data from your Amazon EC2 instance

By creating a MariaDB or MySQL DB instance in the same AWS Region as your Amazon EC2 instance, you can import the database backup file from EC2 faster than over the internet.



To create a MariaDB or MySQL DB instance and import your data

1. Determine which DB instance class and what amount of storage space is required to support the expected workload for this Amazon RDS DB instance. As part of this process, decide what is sufficient space and processing capacity for your data load procedures. Also decide what is required to handle the production workload. You can estimate this based on the size and resources of the source MariaDB or MySQL database. For more information, see [DB instance classes \(p. 10\)](#).
2. Determine if Amazon RDS provisioned I/O operations per second (IOPS) is required to support the workloads. Provisioned IOPS storage delivers fast throughput for online transaction processing (OLTP) workloads, which are I/O intensive. For more information, see [Provisioned IOPS SSD storage \(p. 66\)](#).
3. Open the [Amazon RDS console](#). In the upper-right corner, choose the AWS Region that contains your Amazon EC2 instance.
4. In the navigation pane, choose **Databases**.
5. Choose **Create database**, and then go through the steps to choose options for your DB instance:
 - a. Make sure that **Standard Create** is chosen.
 - b. In the **Engine options** section, choose **MySQL** or **MariaDB**, as appropriate.
 - c. For **Version**, choose the version that is compatible with your source MySQL instance, as follows:
 - If your source instance is MySQL 5.5.x, the Amazon RDS DB instance must be MySQL.
 - If your source instance is MySQL 5.6.x or 5.7.x, the Amazon RDS DB instance must be MySQL or MariaDB.
 - If your source instance is MySQL 8.0.x, the Amazon RDS DB instance must be MySQL 8.0.x.
 - If your source instance is MariaDB 5.5 or higher, the Amazon RDS DB instance must be MariaDB.
 - d. In the **Templates** section, choose **Dev/Test** to skip configuring Multi-AZ deployment and provisioned IOPS storage.
 - e. In the **Settings** section, specify the requested **DB instance identifier** and user information.
 - f. In the **DB instance class** and **Storage** sections, specify the DB instance class and allocated storage size that you want.
 - g. In the **Availability & durability** section, choose **Do not create a standby instance for Multi-AZ deployment**.
 - h. In the **Connectivity** section, choose the same virtual private cloud (VPC) and VPC security group as for your Amazon EC2 instance. This approach ensures that your Amazon EC2 instance and your Amazon RDS instance are visible to each other over the network. Set **Publicly accessible** to **Yes**. To set up replication with your source database as described later, your DB instance must be publicly accessible.

Use the default values for the other settings in this section.

In the **Backup** section, set the backup retention period to **0 days**.

Use the default values for the other settings in this section.

- i. Open the **Additional configuration** section, and specify an **Initial database name**.

Set the **Backup retention period** to **0 days**

Use the default values for the other settings in this section.

- j. Choose **Create database**.

Your new DB instance appears in the **Databases** list with the status **Creating**. Wait for the **Status** of your new DB instance to show as **Available**.

Don't configure multiple Availability Zones, backup retention, or read replicas until after you have imported the database backup. When that import is done, you can set Multi-AZ and backup retention the way that you want them for the production instance. For a detailed walkthrough of creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

6. Review the default configuration options for the Amazon RDS DB instance. In the RDS console navigation pane, choose **Parameter groups**, and then choose the magnifying glass icon next to the **default.mysqlx.x** or **default.mariadb.x** parameter group. If this parameter group doesn't have the configuration options that you want, find a different one that does or create a new parameter group. For more information on creating a parameter group, see [Working with parameter groups \(p. 289\)](#).

To use a different parameter group than the default, associate it with your Amazon RDS DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

7. Connect to the new Amazon RDS DB instance as the master user. Create the users required to support the administrators, applications, and services that need to access the instance. The host name for the Amazon RDS DB instance is the **Endpoint** value for this instance without including the port number. An example is `mysampledb.claxc2oy9ak1.us-west-2.rds.amazonaws.com`. You can find the endpoint value in the instance details in the Amazon RDS Management Console.
8. Connect to your Amazon EC2 instance. For more information, see [Connect to your instance](#) in the *Amazon Elastic Compute Cloud User Guide for Linux*.
9. Connect to your Amazon RDS DB instance as a remote host from your Amazon EC2 instance using the `mysql` command. The following is an example.

```
mysql -h host_name -P 3306 -u db_master_user -p
```

The host name is the DNS name from the Amazon RDS DB instance endpoint.

10. At the `mysql` prompt, run the `source` command and pass it the name of your database dump file to load the data into the Amazon RDS DB instance:
 - For SQL format, use the following command.

```
mysql> source backup.sql;
```

- For delimited-text format, first create the database, if it isn't the default database you created when setting up the Amazon RDS DB instance.

```
mysql> create database database_name;
$ mysql> use database_name;
```

Then create the tables.

```
mysql> source table1.sql
$ mysql> source table2.sql
etc...
```

Then import the data.

```
mysql> LOAD DATA LOCAL INFILE 'table1.txt' INTO TABLE table1 FIELDS TERMINATED BY ',' 
ENCLOSED BY ''' LINES TERMINATED BY '0x0d0a';
$ mysql> LOAD DATA LOCAL INFILE 'table2.txt' INTO TABLE table2 FIELDS TERMINATED BY ',' 
ENCLOSED BY ''' LINES TERMINATED BY '0x0d0a';
etc...
```

To improve performance, you can perform these operations in parallel from multiple connections so that all of your tables get created and then loaded at the same time.

Note

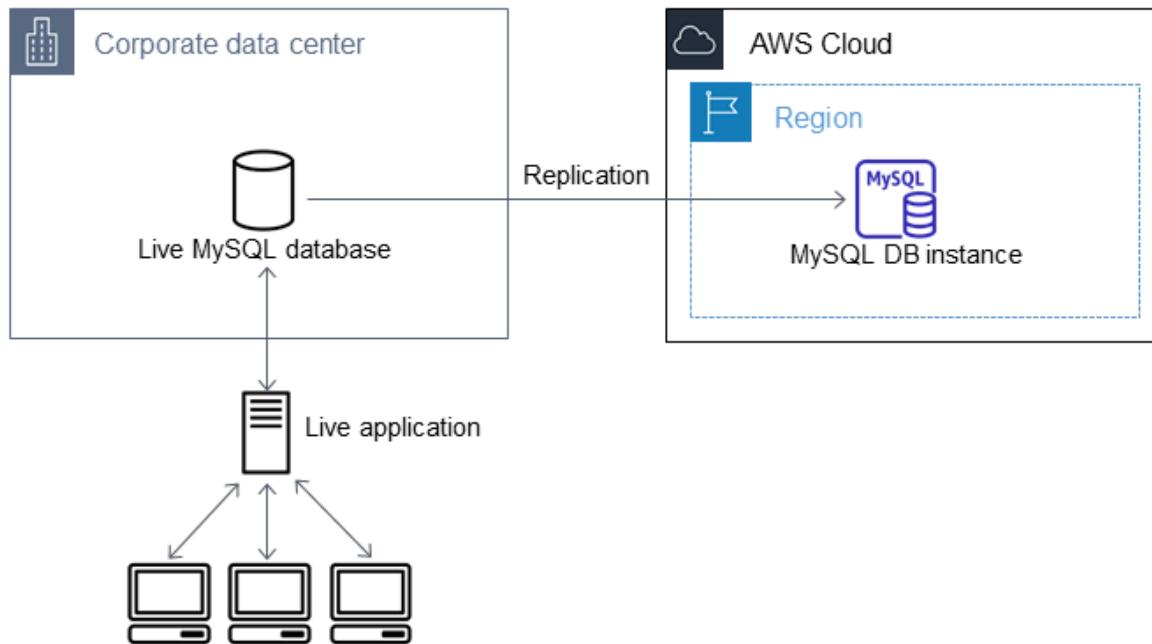
If you used any data-formatting options with `mysqldump` when you initially dumped the table, make sure to use the same options with `mysqlimport` or `LOAD DATA LOCAL INFILE` to ensure proper interpretation of the data file contents.

11. Run a simple `SELECT` query against one or two of the tables in the imported database to verify that the import was successful.

If you no longer need the Amazon EC2 instance used in this procedure, terminate the EC2 instance to reduce your AWS resource usage. To terminate an EC2 instance, see [Terminating an instance](#) in the *Amazon EC2 User Guide*.

Replicate between your external database and new Amazon RDS DB instance

Your source database was likely updated during the time that it took to copy and transfer the data to the MariaDB or MySQL DB instance. That being the case, you can use replication to bring the copied database up-to-date with the source database.



The permissions required to start replication on an Amazon RDS DB instance are restricted and not available to your Amazon RDS master user. Because of this, make sure to use either the Amazon RDS [`mysql.rds_set_external_master` \(p. 1441\)](#) command or the [`mysql.rds_set_external_master_gtid` \(p. 1050\)](#) command to configure replication, and the [`mysql.rds_start_replication` \(p. 1452\)](#) command to start replication between your live database and your Amazon RDS database.

To start replication

Earlier, you turned on binary logging and set a unique server ID for your source database. Now you can set up your Amazon RDS DB instance as a replica with your live database as the source replication instance.

1. In the Amazon RDS Management Console, add the IP address of the server that hosts the source database to the VPC security group for the Amazon RDS DB instance. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.

You might also need to configure your local network to permit connections from the IP address of your Amazon RDS DB instance, so that it can communicate with your source instance. To find the IP address of the Amazon RDS DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the Amazon RDS DB instance endpoint, for example myinstance.123456789012.us-east-1.rds.amazonaws.com. You can find the endpoint value in the instance details in the Amazon RDS Management Console.

2. Using the client of your choice, connect to the source instance and create a user to be used for replication. This account is used solely for replication and must be restricted to your domain to improve security. The following is an example.

MySQL 5.5, 5.6, and 5.7

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

MySQL 8.0

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY 'password';
```

3. For the source instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

MySQL 5.5, 5.6, and 5.7

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'  
IDENTIFIED BY 'password';
```

MySQL 8.0

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

4. If you used SQL format to create your backup file and the external instance is not MariaDB 10.0.24 or higher, look at the contents of that file.

```
cat backup.sql
```

The file includes a CHANGE MASTER TO comment that contains the master log file name and position. This comment is included in the backup file when you use the --master-data option with mysqldump. Note the values for MASTER_LOG_FILE and MASTER_LOG_POS.

```
--  
-- Position to start replication or point-in-time recovery from  
--  
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

If you used delimited text format to create your backup file and the external instance isn't MariaDB 10.0.24 or higher, you should already have binary log coordinates from step 1 of the procedure at "To create a backup copy of your existing database" in this topic.

If the external instance is MariaDB 10.0.24 or higher, you should already have the GTID from which to start replication from step 2 of the procedure at "To create a backup copy of your existing database" in this topic.

5. Make the Amazon RDS DB instance the replica. If the external instance isn't MariaDB 10.0.24 or higher, connect to the Amazon RDS DB instance as the master user and identify the source database as the source replication instance by using the [mysql.rds_set_external_master \(p. 1441\)](#) command. Use the master log file name and master log position that you determined in the previous step if you have a SQL format backup file. Or use the name and position that you determined when creating the backup files if you used delimited-text format. The following is an example.

```
CALL mysql.rds_set_external_master ('myserver.mydomain.com', 3306,  
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 0);
```

If the external instance is MariaDB 10.0.24 or higher, connect to the Amazon RDS DB instance as the master user and identify the source database as the source replication instance by using the [mysql.rds_set_external_master_gtid \(p. 1050\)](#) command. Use the GTID that you determined in step 2 of the procedure at "To create a backup copy of your existing database" in this topic.. The following is an example.

```
CALL mysql.rds_set_external_master_gtid ('source_server_ip_address', 3306,  
    'ReplicationUser', 'password', 'GTID', 0);
```

The `source_server_ip_address` is the IP address of source replication instance. An EC2 private DNS address is currently not supported.

6. On the Amazon RDS DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

7. On the Amazon RDS DB instance, run the [SHOW REPLICAS STATUS](#) command to determine when the replica is up-to-date with the source replication instance. The results of the SHOW REPLICAS STATUS command include the Seconds_Behind_Master field. When the Seconds_Behind_Master field returns 0, then the replica is up-to-date with the source replication instance.

Note

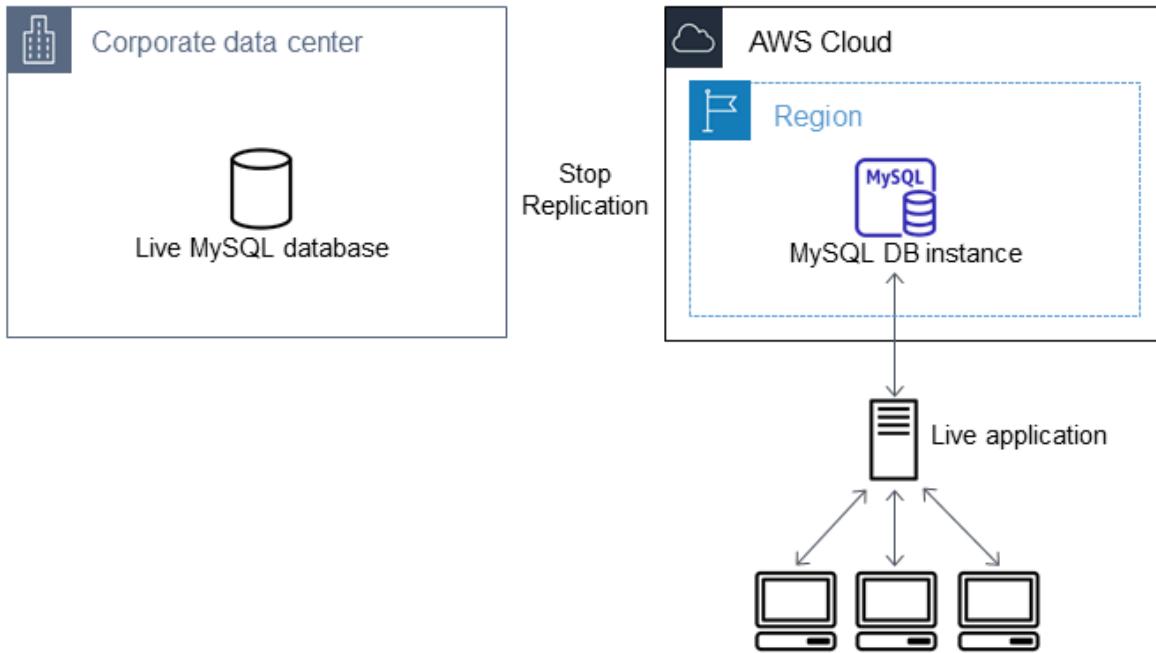
Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICAS STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

For a MariaDB 10.5 or 10.6 DB instance, run the [mysql.rds_replica_status \(p. 1049\)](#) procedure instead of the MySQL command.

8. After the Amazon RDS DB instance is up-to-date, turn on automated backups so you can restore that database if needed. You can turn on or modify automated backups for your Amazon RDS DB instance using the [Amazon RDS Management Console](#). For more information, see [Working with backups \(p. 427\)](#).

Redirect your live application to your Amazon RDS instance

After the MariaDB or MySQL DB instance is up-to-date with the source replication instance, you can now update your live application to use the Amazon RDS instance.



To redirect your live application to your MariaDB or MySQL DB instance and stop replication

1. To add the VPC security group for the Amazon RDS DB instance, add the IP address of the server that hosts the application. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.
2. Verify that the Seconds_Behind_Master field in the [SHOW REPLICAS STATUS](#) command results is 0, which indicates that the replica is up-to-date with the source replication instance.

```
SHOW REPLICAS STATUS;
```

Note

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICAS STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

For a MariaDB 10.5 or 10.6 DB instance, run the [mysql.rds_replica_status \(p. 1049\)](#) procedure instead of the MySQL command.

3. Close all connections to the source when their transactions complete.
4. Update your application to use the Amazon RDS DB instance. This update typically involves changing the connection settings to identify the host name and port of the Amazon RDS DB instance, the user account and password to connect with, and the database to use.
5. Stop replication for the Amazon RDS instance using the [mysql.rds_stop_replication \(p. 1454\)](#) command.

```
CALL mysql.rds_stop_replication;
```

6. Run the [mysql.rds_reset_external_master \(p. 1448\)](#) command on your Amazon RDS DB instance to reset the replication configuration so this instance is no longer identified as a replica.

```
CALL mysql.rds_reset_external_master;
```

7. Turn on additional Amazon RDS features such as Multi-AZ support and read replicas. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#) and [Working with read replicas \(p. 370\)](#).

Importing data from any source to a MariaDB or MySQL DB instance

If you have more than 1 GiB of data to load, or if your data is coming from somewhere other than a MariaDB or MySQL database, we recommend creating flat files and loading them with mysqlimport. The mysqlimport utility is another command line utility bundled with the MySQL and MariaDB client software. Its purpose is to load flat files into MySQL or MariaDB. For information about mysqlimport, see [mysqlimport - a data import program](#) in the MySQL documentation.

We also recommend creating DB snapshots of the target Amazon RDS DB instance before and after the data load. Amazon RDS DB snapshots are complete backups of your DB instance that can be used to restore your DB instance to a known state. When you initiate a DB snapshot, I/O operations to your DB instance are momentarily suspended while your database is backed up.

Creating a DB snapshot immediately before the load makes it possible for you to restore the database to its state before the load, if you need to. A DB snapshot taken immediately after the load protects you from having to load the data again in case of a mishap and can also be used to seed new database instances.

The following list shows the steps to take. Each step is discussed in more detail following.

1. Create flat files containing the data to be loaded.
2. Stop any applications accessing the target DB instance.
3. Create a DB snapshot.
4. Consider turning off Amazon RDS automated backups.
5. Load the data using mysqlimport.
6. Enable automated backups again.

Step 1: Create flat files containing the data to be loaded

Use a common format, such as comma-separated values (CSV), to store the data to be loaded. Each table must have its own file; you can't combine data for multiple tables in the same file. Give each file the same name as the table it corresponds to. The file extension can be anything you like. For example, if the table name is sales, the file name might be sales.csv or sales.txt, but not sales_01.csv.

Whenever possible, order the data by the primary key of the table being loaded. Doing this drastically improves load times and minimizes disk storage requirements.

The speed and efficiency of this procedure depends on keeping the size of the files small. If the uncompressed size of any individual file is larger than 1 GiB, split it into multiple files and load each one separately.

On Unix-like systems (including Linux), use the `split` command. For example, the following command splits the sales.csv file into multiple files of less than 1 GiB, splitting only at line breaks (-C 1024m). The new files are named sales.part_00, sales.part_01, and so on.

```
split -C 1024m -d sales.csv sales.part_
```

Similar utilities are available for other operating systems.

Step 2: Stop any applications accessing the target DB instance

Before starting a large load, stop all application activity accessing the target DB instance that you plan to load to. We recommend this particularly if other sessions will be modifying the tables being loaded or tables that they reference. Doing this reduces the risk of constraint violations occurring during the load and improves load performance. It also makes it possible to restore the DB instance to the point just before the load without losing changes made by processes not involved in the load.

Of course, this might not be possible or practical. If you can't stop applications from accessing the DB instance before the load, take steps to ensure the availability and integrity of your data. The specific steps required vary greatly depending upon specific use cases and site requirements.

Step 3: Create a DB snapshot

If you plan to load data into a new DB instance that contains no data, you can skip this step. Otherwise, creating a DB snapshot of your DB instance makes it possible for you to restore the DB instance to the point just before the load, if it becomes necessary. As previously mentioned, when you initiate a DB snapshot, I/O operations to your DB instance are suspended for a few minutes while the database is backed up.

The example following uses the AWS CLI `create-db-snapshot` command to create a DB snapshot of the AcmeRDS instance and give the DB snapshot the identifier "preload".

For Linux, macOS, or Unix:

```
aws rds create-db-snapshot \  
  --db-instance-identifier AcmeRDS \  
  --db-snapshot-identifier preload
```

For Windows:

```
aws rds create-db-snapshot ^  
  --db-instance-identifier AcmeRDS ^  
  --db-snapshot-identifier preload
```

You can also use the restore from DB snapshot functionality to create test DB instances for dry runs or to undo changes made during the load.

Keep in mind that restoring a database from a DB snapshot creates a new DB instance that, like all DB instances, has a unique identifier and endpoint. To restore the DB instance without changing the endpoint, first delete the DB instance so that you can reuse the endpoint.

For example, to create a DB instance for dry runs or other testing, you give the DB instance its own identifier. In the example, `AcmeRDS-2` is the identifier. The example connects to the DB instance using the endpoint associated with `AcmeRDS-2`.

For Linux, macOS, or Unix:

```
aws rds restore-db-instance-from-db-snapshot \  
  --db-instance-identifier AcmeRDS-2 \  
  --db-snapshot-identifier preload
```

For Windows:

```
aws rds restore-db-instance-from-db-snapshot ^  
  --db-instance-identifier AcmeRDS-2 ^
```

```
--db-snapshot-identifier preload
```

To reuse the existing endpoint, first delete the DB instance and then give the restored database the same identifier.

For Linux, macOS, or Unix:

```
aws rds delete-db-instance \  
  --db-instance-identifier AcmeRDS \  
  --final-db-snapshot-identifier AcmeRDS-Final  
  
aws rds restore-db-instance-from-db-snapshot \  
  --db-instance-identifier AcmeRDS \  
  --db-snapshot-identifier preload
```

For Windows:

```
aws rds delete-db-instance ^  
  --db-instance-identifier AcmeRDS ^  
  --final-db-snapshot-identifier AcmeRDS-Final  
  
aws rds restore-db-instance-from-db-snapshot ^  
  --db-instance-identifier AcmeRDS ^  
  --db-snapshot-identifier preload
```

The preceding example takes a final DB snapshot of the DB instance before deleting it. This is optional but recommended.

Step 4: Consider turning off Amazon RDS automated backups

Warning

Do not turn off automated backups if you need to perform point-in-time recovery.

Turning off automated backups erases all existing backups, so point-in-time recovery isn't possible after automated backups have been turned off. Disabling automated backups is a performance optimization and isn't required for data loads. Manual DB snapshots aren't affected by turning off automated backups. All existing manual DB snapshots are still available for restore.

Turning off automated backups reduces load time by about 25 percent and reduces the amount of storage space required during the load. If you plan to load data into a new DB instance that contains no data, turning off backups is an easy way to speed up the load and avoid using the additional storage needed for backups. However, in some cases you might plan to load into a DB instance that already contains data. If so, weigh the benefits of turning off backups against the impact of losing the ability to perform point-in-time-recovery.

DB instances have automated backups turned on by default (with a one day retention period). To turn off automated backups, set the backup retention period to zero. After the load, you can turn backups back on by setting the backup retention period to a nonzero value. To turn on or turn off backups, Amazon RDS shuts the DB instance down and restarts it to turn MariaDB or MySQL logging on or off.

Use the AWS CLI `modify-db-instance` command to set the backup retention to zero and apply the change immediately. Setting the retention period to zero requires a DB instance restart, so wait until the restart has completed before proceeding.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \  
  --db-instance-identifier AcmeRDS \  
  --backup-retention 0
```

```
--apply-immediately \
--backup-retention-period 0
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier AcmeRDS ^
--apply-immediately ^
--backup-retention-period 0
```

You can check the status of your DB instance with the AWS CLI `describe-db-instances` command. The following example displays the DB instance status of the AcmeRDS DB instance.

```
aws rds describe-db-instances --db-instance-identifier AcmeRDS --query "[].{DBInstanceState:DBInstanceState}"
```

When the DB instance status is available, you're ready to proceed.

Step 5: Load the data

Use the `mysqlimport` utility to load the flat files into Amazon RDS. The following example tells `mysqlimport` to load all of the files named "sales" with an extension starting with "part_". This is a convenient way to load all of the files created in the "split" example.

Use the `--compress` option to minimize network traffic. The `--fields-terminated-by=','` option is used for CSV files, and the `--local` option specifies that the incoming data is located on the client. Without the `--local` option, the Amazon RDS DB instance looks for the data on the database host, so always specify the `--local` option. For the `--host` option, specify the DB instance endpoint of the RDS for MySQL DB instance.

In the following examples, replace `master_user` with the master username for your DB instance.

Replace `hostname` with the endpoint for your DB instance. An example of a DB instance endpoint is `my-db-instance.123456789012.us-west-2.rds.amazonaws.com`.

For RDS for MySQL version 8.0.15 and higher, run the following statement before using the `mysqlimport` utility.

```
GRANT SESSION_VARIABLES_ADMIN ON *.* TO master_user;
```

For Linux, macOS, or Unix:

```
mysqlimport --local \
--compress \
--user=master_user \
--password \
--host=hostname \
--fields-terminated-by=',' Acme sales.part_*
```

For Windows:

```
mysqlimport --local ^
--compress ^
--user=master_user ^
--password ^
--host=hostname ^
--fields-terminated-by="," Acme sales.part_*
```

For very large data loads, take additional DB snapshots periodically between loading files and note which files have been loaded. If a problem occurs, you can easily resume from the point of the last DB snapshot, avoiding lengthy reloads.

Step 6: Turn Amazon RDS automated backups back on

After the load is finished, turn Amazon RDS automated backups on by setting the backup retention period back to its preload value. As noted earlier, Amazon RDS restarts the DB instance, so be prepared for a brief outage.

The following example uses the AWS CLI `modify-db-instance` command to turn on automated backups for the AcmeRDS DB instance and set the retention period to one day.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier AcmeRDS \
--backup-retention-period 1 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier AcmeRDS ^
--backup-retention-period 1 ^
--apply-immediately
```

Working with MySQL replication in Amazon RDS

You usually use read replicas to configure replication between Amazon RDS DB instances. For general information about read replicas, see [Working with read replicas \(p. 370\)](#). For specific information about working with read replicas on Amazon RDS for MySQL, see [Working with MySQL read replicas \(p. 1389\)](#).

You can use global transaction identifiers (GTIDs) for replication with RDS for MySQL. For more information, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

You can also set up replication between an RDS for MySQL DB instance and a MariaDB or MySQL instance that is external to Amazon RDS. For information about configuring replication with an external source, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#).

For any of these replication options, you can use either row-based replication, statement-based, or mixed replication. Row-based replication only replicates the changed rows that result from a SQL statement. Statement-based replication replicates the entire SQL statement. Mixed replication uses statement-based replication when possible, but switches to row-based replication when SQL statements that are unsafe for statement-based replication are run. In most cases, mixed replication is recommended. The binary log format of the DB instance determines whether replication is row-based, statement-based, or mixed. For information about setting the binary log format, see [Configuring MySQL binary logging \(p. 706\)](#).

Note

You can configure replication to import databases from a MariaDB or MySQL instance that is external to Amazon RDS, or to export databases to such instances. For more information, see [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#) and [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

Topics

- [Working with MySQL read replicas \(p. 1389\)](#)
- [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#)
- [Configuring GTID-based replication with an external source instance \(p. 1405\)](#)
- [Configuring binary log file position replication with an external source instance \(p. 1408\)](#)

Working with MySQL read replicas

Following, you can find specific information about working with read replicas on RDS for MySQL. For general information about read replicas and instructions for using them, see [Working with read replicas \(p. 370\)](#).

Topics

- [Configuring read replicas with MySQL \(p. 1390\)](#)
- [Configuring replication filters with MySQL \(p. 1390\)](#)
- [Configuring delayed replication with MySQL \(p. 1395\)](#)
- [Updating read replicas with MySQL \(p. 1397\)](#)
- [Working with Multi-AZ read replica deployments with MySQL \(p. 1397\)](#)
- [Using cascading read replicas with RDS for MySQL \(p. 1398\)](#)
- [Monitoring MySQL read replicas \(p. 1398\)](#)
- [Starting and stopping replication with MySQL read replicas \(p. 1399\)](#)
- [Troubleshooting a MySQL read replica problem \(p. 1399\)](#)

Configuring read replicas with MySQL

Before a MySQL DB instance can serve as a replication source, make sure to enable automatic backups on the source DB instance. To do this, set the backup retention period to a value other than 0. This requirement also applies to a read replica that is the source DB instance for another read replica. Automatic backups are supported for read replicas running any version of MySQL. You can configure replication based on binary log coordinates for a MySQL DB instance.

On RDS for MySQL version 5.7.23 and higher MySQL 5.7 versions and RDS for MySQL 8.0.26 and higher 8.0 versions, you can configure replication using global transaction identifiers (GTIDs). For more information, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

You can create up to 15 read replicas from one DB instance within the same Region. For replication to operate effectively, each read replica should have the same amount of compute and storage resources as the source DB instance. If you scale the source DB instance, also scale the read replicas.

RDS for MySQL supports cascading read replicas. To learn how to configure cascading read replicas, see [Using cascading read replicas with RDS for MySQL \(p. 1398\)](#).

You can run multiple read replica create and delete actions at the same time that reference the same source DB instance. When you perform these actions, stay within the limit of 15 read replicas for each source instance.

A read replica of a MySQL DB instance can't use a lower DB engine version than its source DB instance.

Preparing MySQL DB instances that use MyISAM

If your MySQL DB instance uses a nontransactional engine such as MyISAM, you need to perform the following steps to successfully set up your read replica. These steps are required to make sure that the read replica has a consistent copy of your data. These steps are not required if all of your tables use a transactional engine such as InnoDB.

1. Stop all data manipulation language (DML) and data definition language (DDL) operations on non-transactional tables in the source DB instance and wait for them to complete. SELECT statements can continue running.
2. Flush and lock the tables in the source DB instance.
3. Create the read replica using one of the methods in the following sections.
4. Check the progress of the read replica creation using, for example, the `DescribeDBInstances` API operation. Once the read replica is available, unlock the tables of the source DB instance and resume normal database operations.

Configuring replication filters with MySQL

You can use replication filters to specify which databases and tables are replicated with a read replica. Replication filters can include databases and tables in replication or exclude them from replication.

The following are some use cases for replication filters:

- To reduce the size of a read replica. With replication filtering, you can exclude the databases and tables that aren't needed on the read replica.
- To exclude databases and tables from read replicas for security reasons.
- To replicate different databases and tables for specific use cases at different read replicas. For example, you might use specific read replicas for analytics or sharding.
- For a DB instance that has read replicas in different AWS Regions, to replicate different databases or tables in different AWS Regions.

Note

You can also use replication filters to specify which databases and tables are replicated with a primary MySQL DB instance that is configured as a replica in an inbound replication topology. For more information about this configuration, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#).

Topics

- [Setting replication filtering parameters for RDS for MySQL \(p. 1391\)](#)
- [Replication filtering limitations for RDS for MySQL \(p. 1392\)](#)
- [Replication filtering examples for RDS for MySQL \(p. 1392\)](#)
- [Viewing the replication filters for a read replica \(p. 1395\)](#)

Setting replication filtering parameters for RDS for MySQL

To configure replication filters, set the following replication filtering parameters on the read replica:

- `replicate-do-db` – Replicate changes to the specified databases. When you set this parameter for a read replica, only the databases specified in the parameter are replicated.
- `replicate-ignore-db` – Don't replicate changes to the specified databases. When the `replicate-do-db` parameter is set for a read replica, this parameter isn't evaluated.
- `replicate-do-table` – Replicate changes to the specified tables. When you set this parameter for a read replica, only the tables specified in the parameter are replicated. Also, when the `replicate-do-db` or `replicate-ignore-db` parameter is set, make sure to include the database that includes the specified tables in replication with the read replica.
- `replicate-ignore-table` – Don't replicate changes to the specified tables. When the `replicate-do-table` parameter is set for a read replica, this parameter isn't evaluated.
- `replicate-wild-do-table` – Replicate tables based on the specified database and table name patterns. The % and _ wildcard characters are supported. When the `replicate-do-db` or `replicate-ignore-db` parameter is set, make sure to include the database that includes the specified tables in replication with the read replica.
- `replicate-wild-ignore-table` – Don't replicate tables based on the specified database and table name patterns. The % and _ wildcard characters are supported. When the `replicate-do-table` or `replicate-wild-do-table` parameter is set for a read replica, this parameter isn't evaluated.

The parameters are evaluated in the order that they are listed. For more information about how these parameters work, see the MySQL documentation:

- For general information, see [Replica Server Options and Variables](#).
- For information about how database replication filtering parameters are evaluated, see [Evaluation of Database-Level Replication and Binary Logging Options](#).
- For information about how table replication filtering parameters are evaluated, see [Evaluation of Table-Level Replication Options](#).

By default, each of these parameters has an empty value. On each read replica, you can use these parameters to set, change, and delete replication filters. When you set one of these parameters, separate each filter from others with a comma.

You can use the % and _ wildcard characters in the `replicate-wild-do-table` and `replicate-wild-ignore-table` parameters. The % wildcard matches any number of characters, and the _ wildcard matches only one character.

The binary logging format of the source DB instance is important for replication because it determines the record of data changes. The setting of the `binlog_format` parameter determines whether the

replication is row-based or statement-based. For more information, see [Configuring MySQL binary logging \(p. 706\)](#).

Note

All data definition language (DDL) statements are replicated as statements, regardless of the binlog_format setting on the source DB instance.

Replication filtering limitations for RDS for MySQL

The following limitations apply to replication filtering for RDS for MySQL:

- Each replication filtering parameter has a 2,000-character limit.
- Commas aren't supported in replication filters.
- The MySQL --binlog-do-db and --binlog-ignore-db options for binary log filtering aren't supported.
- Replication filtering doesn't support XA transactions.

For more information, see [Restrictions on XA Transactions](#) in the MySQL documentation.

Replication filtering examples for RDS for MySQL

To configure replication filtering for a read replica, modify the replication filtering parameters in the parameter group associated with the read replica.

Note

You can't modify a default parameter group. If the read replica is using a default parameter group, create a new parameter group and associate it with the read replica. For more information on DB parameter groups, see [Working with parameter groups \(p. 289\)](#).

You can set parameters in a parameter group using the AWS Management Console, AWS CLI, or RDS API. For information about setting parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#). When you set parameters in a parameter group, all of the DB instances associated with the parameter group use the parameter settings. If you set the replication filtering parameters in a parameter group, make sure that the parameter group is associated only with read replicas. Leave the replication filtering parameters empty for source DB instances.

The following examples set the parameters using the AWS CLI. These examples set ApplyMethod to immediate so that the parameter changes occur immediately after the CLI command completes. If you want a pending change to be applied after the read replica is rebooted, set ApplyMethod to pending-reboot.

The following examples set replication filters:

- [Including databases in replication](#)
- [Including tables in replication](#)
- [Including tables in replication with wildcard characters](#)
- [Escaping wildcard characters in names](#)
- [Excluding databases from replication](#)
- [Excluding tables from replication](#)
- [Excluding tables from replication using wildcard characters](#)

Example Including databases in replication

The following example includes the mydb1 and mydb2 databases in replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
"ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
"ApplyMethod":"immediate"}]"
```

Example Including tables in replication

The following example includes the `table1` and `table2` tables in database `mydb1` in replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-do-table", "ParameterValue": "mydb1.table1,mydb1.table2",
"ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-do-table", "ParameterValue": "mydb1.table1,mydb1.table2",
"ApplyMethod":"immediate"}]"
```

Example Including tables in replication using wildcard characters

The following example includes tables with names that begin with `orders` and `returns` in database `mydb` in replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "mydb.orders%,mydb>Returns%",
"ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "mydb.orders%,mydb>Returns%",
"ApplyMethod":"immediate"}]"
```

Example Escaping wildcard characters in names

The following example shows you how to use the escape character `\` to escape a wildcard character that is part of a name.

Assume that you have several table names in database mydb1 that start with `my_table`, and you want to include these tables in replication. The table names include an underscore, which is also a wildcard character, so the example escapes the underscore in the table names.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my\_\_table%", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my\_\_table%", "ApplyMethod":"immediate"}]"
```

Example Excluding databases from replication

The following example excludes the `mydb1` and `mydb2` databases from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue": "mydb1,mydb2", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue": "mydb1,mydb2", "ApplyMethod":"immediate"}]"
```

Example Excluding tables from replication

The following example excludes tables `table1` and `table2` in database `mydb1` from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue": "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue": "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

Example Excluding tables from replication using wildcard characters

The following example excludes tables with names that begin with `orders` and `returns` in database `mydb` from replication.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name myparametergroup ^
--parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue": "mydb.orders%,mydb_returns%", "ApplyMethod":"immediate"}]"
```

Viewing the replication filters for a read replica

You can view the replication filters for a read replica in the following ways:

- Check the settings of the replication filtering parameters in the parameter group associated with the read replica.

For instructions, see [Viewing parameter values for a DB parameter group \(p. 301\)](#).

- In a MySQL client, connect to the read replica and run the `SHOW REPLICA STATUS` statement.

In the output, the following fields show the replication filters for the read replica:

- `Replicate_Do_DB`
- `Replicate_Ignore_DB`
- `Replicate_Do_Table`
- `Replicate_Ignore_Table`
- `Replicate_Wild_Do_Table`
- `Replicate_Wild_Ignore_Table`

For more information about these fields, see [Checking Replication Status](#) in the MySQL documentation.

Note

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICA STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

Configuring delayed replication with MySQL

You can use delayed replication as a strategy for disaster recovery. With delayed replication, you specify the minimum amount of time, in seconds, to delay replication from the source to the read replica. In the event of a disaster, such as a table deleted unintentionally, you complete the following steps to recover from the disaster quickly:

- Stop replication to the read replica before the change that caused the disaster is sent to it.

Use the [mysql.rds_stop_replication \(p. 1454\)](#) stored procedure to stop replication.

- Start replication and specify that replication stops automatically at a log file location.
You specify a location just before the disaster using the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure.
- Promote the read replica to be the new source DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Note

- On RDS for MySQL 8.0, delayed replication is supported for MySQL 8.0.26 and higher. On RDS for MySQL 5.7, delayed replication is supported for MySQL 5.7.22 and higher.
- Use stored procedures to configure delayed replication. You can't configure delayed replication with the AWS Management Console, the AWS CLI, or the Amazon RDS API.
- On RDS for MySQL 5.7.23 and higher MySQL 5.7 versions and RDS for MySQL 8.0.26 and higher 8.0 versions, you can use replication based on global transaction identifiers (GTIDs) in a delayed replication configuration. If you use GTID-based replication, use the [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure instead of the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure. For more information about GTID-based replication, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

Topics

- [Configuring delayed replication during read replica creation \(p. 1396\)](#)
- [Modifying delayed replication for an existing read replica \(p. 1396\)](#)
- [Setting a location to stop replication to a read replica \(p. 1397\)](#)
- [Promoting a read replica \(p. 1397\)](#)

Configuring delayed replication during read replica creation

To configure delayed replication for any future read replica created from a DB instance, run the [mysql.rds_set_configuration \(p. 1459\)](#) stored procedure with the `target_delay` parameter.

To configure delayed replication during read replica creation

1. Using a MySQL client, connect to the MySQL DB instance to be the source for read replicas as the master user.
2. Run the [mysql.rds_set_configuration \(p. 1459\)](#) stored procedure with the `target_delay` parameter.

For example, run the following stored procedure to specify that replication is delayed by at least one hour (3,600 seconds) for any read replica created from the current DB instance.

```
call mysql.rds_set_configuration('target_delay', 3600);
```

Note

After running this stored procedure, any read replica you create using the AWS CLI or Amazon RDS API is configured with replication delayed by the specified number of seconds.

Modifying delayed replication for an existing read replica

To modify delayed replication for an existing read replica, run the [mysql.rds_set_source_delay \(p. 1451\)](#) stored procedure.

To modify delayed replication for an existing read replica

1. Using a MySQL client, connect to the read replica as the master user.
2. Use the [mysql.rds_stop_replication \(p. 1454\)](#) stored procedure to stop replication.
3. Run the [mysql.rds_set_source_delay \(p. 1451\)](#) stored procedure.

For example, run the following stored procedure to specify that replication to the read replica is delayed by at least one hour (3600 seconds).

```
call mysql.rds_set_source_delay(3600);
```

4. Use the [mysql.rds_start_replication \(p. 1452\)](#) stored procedure to start replication.

Setting a location to stop replication to a read replica

After stopping replication to the read replica, you can start replication and then stop it at a specified binary log file location using the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure.

To start replication to a read replica and stop replication at a specific location

1. Using a MySQL client, connect to the source MySQL DB instance as the master user.
2. Run the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure.

The following example initiates replication and replicates changes until it reaches location 120 in the `mysql-bin-changelog.000777` binary log file. In a disaster recovery scenario, assume that location 120 is just before the disaster.

```
call mysql.rds_start_replication_until(
    'mysql-bin-changelog.000777',
    120);
```

Replication stops automatically when the stop point is reached. The following RDS event is generated: `Replication has been stopped since the replica reached the stop point specified by the rds_start_replication_until stored procedure.`

Promoting a read replica

After replication is stopped, in a disaster recovery scenario, you can promote a read replica to be the new source DB instance. For information about promoting a read replica, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Updating read replicas with MySQL

Read replicas are designed to support read queries, but you might need occasional updates. For example, you might need to add an index to optimize the specific types of queries accessing the replica. You can enable updates by setting the `read_only` parameter to `0` in the DB parameter group for the read replica. Be careful when disabling read-only on a read replica because it can cause problems if the read replica becomes incompatible with the source DB instance. Change the value of the `read_only` parameter back to `1` as soon as possible.

Working with Multi-AZ read replica deployments with MySQL

You can create a read replica from either single-AZ or Multi-AZ DB instance deployments. You use Multi-AZ deployments to improve the durability and availability of critical data, but you can't use the Multi-AZ

secondary to serve read-only queries. Instead, you can create read replicas from high-traffic Multi-AZ DB instances to offload read-only queries. If the source instance of a Multi-AZ deployment fails over to the secondary, any associated read replicas automatically switch to use the secondary (now primary) as their replication source. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

You can create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

Using cascading read replicas with RDS for MySQL

RDS for MySQL supports cascading read replicas. With *cascading read replicas*, you can scale reads without adding overhead to your source RDS for MySQL DB instance.

With cascading read replicas, your RDS for MySQL DB instance sends data to the first read replica in the chain. That read replica then sends data to the second replica in the chain, and so on. The end result is that all read replicas in the chain have the changes from the RDS for MySQL DB instance, but without the overhead solely on the source DB instance.

You can create a series of up to three read replicas in a chain from a source RDS for MySQL DB instance. For example, suppose that you have an RDS for MySQL DB instance, `mysql-main`. You can do the following:

- Starting with `mysql-main`, create the first read replica in the chain, `read-replica-1`.
- Next, from `read-replica-1`, create the next read replica in the chain, `read-replica-2`.
- Finally, from `read-replica-2`, create the third read replica in the chain, `read-replica-3`.

You can't create another read replica beyond this third cascading read replica in the series for `mysql-main`. A complete series of instances from an RDS for MySQL source DB instance through to the end of a series of cascading read replicas can consist of at most four DB instances.

For cascading read replicas to work, each source RDS for MySQL DB instance must have automated backups turned on. To turn on automatic backups on a read replica, first create the read replica, and then modify the read replica to turn on automatic backups. For more information, see [Creating a read replica \(p. 375\)](#).

As with any read replica, you can promote a read replica that's part of a cascade. Promoting a read replica from within a chain of read replicas removes that replica from the chain. For example, suppose that you want to move some of the workload from your `mysql-main` DB instance to a new instance for use by the accounting department only. Assuming the chain of three read replicas from the example, you decide to promote `read-replica-2`. The chain is affected as follows:

- Promoting `read-replica-2` removes it from the replication chain.
 - It is now a full read/write DB instance.
 - It continues replicating to `read-replica-3`, just as it was doing before promotion.
- Your `mysql-main` continues replicating to `read-replica-1`.

For more information about promoting read replicas, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Monitoring MySQL read replicas

For MySQL read replicas, you can monitor replication lag in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric. The ReplicaLag metric reports the value of the Seconds_Behind_Master field of the SHOW REPLICAS STATUS command.

Note

Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

Common causes for replication lag for MySQL are the following:

- A network outage.
- Writing to tables that have different indexes on a read replica. If the `read_only` parameter is set to `0` on the read replica, replication can break if the read replica becomes incompatible with the source DB instance. After you've performed maintenance tasks on the read replica, we recommend that you set the `read_only` parameter back to `1`.
- Using a nontransactional storage engine such as MyISAM. Replication is only supported for the InnoDB storage engine on MySQL.

When the ReplicaLag metric reaches 0, the replica has caught up to the source DB instance. If the ReplicaLag metric returns -1, then replication is currently not active. ReplicaLag = -1 is equivalent to Seconds_Behind_Master = NULL.

Starting and stopping replication with MySQL read replicas

You can stop and restart the replication process on an Amazon RDS DB instance by calling the system stored procedures [mysql.rds_stop_replication \(p. 1454\)](#) and [mysql.rds_start_replication \(p. 1452\)](#). You can do this when replicating between two Amazon RDS instances for long-running operations such as creating large indexes. You also need to stop and start replication when importing or exporting databases. For more information, see [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#) and [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

If replication is stopped for more than 30 consecutive days, either manually or due to a replication error, Amazon RDS terminates replication between the source DB instance and all read replicas. It does so to prevent increased storage requirements on the source DB instance and long failover times. The read replica DB instance is still available. However, replication can't be resumed because the binary logs required by the read replica are deleted from the source DB instance after replication is terminated. You can create a new read replica for the source DB instance to reestablish replication.

Troubleshooting a MySQL read replica problem

For MySQL DB instances, in some cases read replicas present replication errors or data inconsistencies (or both) between the read replica and its source DB instance. This problem occurs when some binary log (binlog) events or InnoDB redo logs aren't flushed during a failure of the read replica or the source DB instance. In these cases, manually delete and recreate the read replicas. You can reduce the chance of this happening by setting the following parameter values: `sync_binlog=1` and `innodb_flush_log_at_trx_commit=1`. These settings might reduce performance, so test their impact before implementing the changes in a production environment.

Warning

In the parameter group associated with the source DB instance, we recommend keeping these parameters values: `sync_binlog=1` and `innodb_flush_log_at_trx_commit=1`. These parameters are dynamic. If you don't want to use these settings, we recommend temporarily setting those values before executing any operation on the source DB instance that might cause it to restart. These operations include, but are not limited to, rebooting, rebooting with failover, upgrading the database version, and changing the DB instance class or its storage. The same recommendation applies to creating new read replicas for the source DB instance.

Failure to follow this guidance increases the risk of read replicas presenting replication errors or data inconsistencies (or both) between the read replica and its source DB instance.

The replication technologies for MySQL are asynchronous. Because they are asynchronous, occasional BinLogDiskUsage increases on the source DB instance and ReplicaLag on the read replica are to be expected. For example, a high volume of write operations to the source DB instance can occur in parallel. In contrast, write operations to the read replica are serialized using a single I/O thread, which can lead to a lag between the source instance and read replica. For more information about read-only replicas in the MySQL documentation, see [Replication implementation details](#).

You can do several things to reduce the lag between updates to a source DB instance and the subsequent updates to the read replica, such as the following:

- Sizing a read replica to have a storage size and DB instance class comparable to the source DB instance.
- Ensuring that parameter settings in the DB parameter groups used by the source DB instance and the read replica are compatible. For more information and an example, see the discussion of the max_allowed_packet parameter later in this section.

Amazon RDS monitors the replication status of your read replicas and updates the Replication State field of the read replica instance to Error if replication stops for any reason. An example might be if DML queries run on your read replica conflict with the updates made on the source DB instance.

You can review the details of the associated error thrown by the MySQL engine by viewing the Replication Error field. Events that indicate the status of the read replica are also generated, including [RDS-EVENT-0045 \(p. 675\)](#), [RDS-EVENT-0046 \(p. 675\)](#), and [RDS-EVENT-0047 \(p. 672\)](#). For more information about events and subscribing to events, see [Working with Amazon RDS event notification \(p. 650\)](#). If a MySQL error message is returned, review the error number in the [MySQL error message documentation](#).

One common issue that can cause replication errors is when the value for the max_allowed_packet parameter for a read replica is less than the max_allowed_packet parameter for the source DB instance. The max_allowed_packet parameter is a custom parameter that you can set in a DB parameter group. You use max_allowed_packet to specify the maximum size of DML code that can be run on the database. In some cases, the max_allowed_packet value in the DB parameter group associated with a read replica is smaller than the max_allowed_packet value in the DB parameter group associated with the source DB instance. In these cases, the replication process can throw the error Packet bigger than 'max_allowed_packet' bytes and stop replication. To fix the error, have the source DB instance and read replica use DB parameter groups with the same max_allowed_packet parameter values.

Other common situations that can cause replication errors include the following:

- Writing to tables on a read replica. In some cases, you might create indexes on a read replica that are different from the indexes on the source DB instance. If you do, set the read_only parameter to 0 to create the indexes. If you write to tables on the read replica, it might break replication if the read replica becomes incompatible with the source DB instance. After you perform maintenance tasks on the read replica, we recommend that you set the read_only parameter back to 1.
- Using a non-transactional storage engine such as MyISAM. Read replicas require a transactional storage engine. Replication is only supported for the InnoDB storage engine on MySQL.
- Using unsafe nondeterministic queries such as SYSDATE(). For more information, see [Determination of safe and unsafe statements in binary logging](#).

If you decide that you can safely skip an error, you can follow the steps described in the section [Skipping the current replication error \(p. 1428\)](#). Otherwise, you can first delete the read replica. Then you create an instance using the same DB instance identifier so that the endpoint remains the same as that of your old read replica. If a replication error is fixed, the Replication State changes to replicating.

Using GTID-based replication for Amazon RDS for MySQL

Following, you can learn how to use global transaction identifiers (GTIDs) with binary log (binlog) replication among Amazon RDS for MySQL DB instances.

If you use binlog replication and aren't familiar with GTID-based replication with MySQL, see [Replication with global transaction identifiers](#) in the MySQL documentation for background.

GTID-based replication is supported for all RDS for MySQL 5.7 versions, and RDS for MySQL version 8.0.26 and higher MySQL 8.0 versions. All MySQL DB instances in a replication configuration must meet this requirement.

Topics

- [Overview of global transaction identifiers \(GTIDs\) \(p. 1401\)](#)
- [Parameters for GTID-based replication \(p. 1401\)](#)
- [Configuring GTID-based replication for new read replicas \(p. 1402\)](#)
- [Configuring GTID-based replication for existing read replicas \(p. 1403\)](#)
- [Disabling GTID-based replication for a MySQL DB instance with read replicas \(p. 1404\)](#)

Note

For information about configuring GTID-based replication with an external database, see [Configuring GTID-based replication with an external source instance \(p. 1405\)](#).

Overview of global transaction identifiers (GTIDs)

Global transaction identifiers (GTIDs) are unique identifiers generated for committed MySQL transactions. You can use GTIDs to make binlog replication simpler and easier to troubleshoot.

MySQL uses two different types of transactions for binlog replication:

- *GTID transactions* – Transactions that are identified by a GTID.
- *Anonymous transactions* – Transactions that don't have a GTID assigned.

In a replication configuration, GTIDs are unique across all DB instances. GTIDs simplify replication configuration because when you use them, you don't have to refer to log file positions. GTIDs also make it easier to track replicated transactions and determine whether the source instance and replicas are consistent.

You can use GTID-based replication to replicate data with RDS for MySQL read replicas. You can configure GTID-based replication when you are creating new read replicas, or you can convert existing read replicas to use GTID-based replication.

You can also use GTID-based replication in a delayed replication configuration with RDS for MySQL. For more information, see [Configuring delayed replication with MySQL \(p. 1395\)](#).

Parameters for GTID-based replication

Use the following parameters to configure GTID-based replication.

Parameter	Valid values	Description
gtid_mode	OFF, OFF_PERMISSIVE, ON_PERMISSIVE, ON	<p>OFF specifies that new transactions are anonymous transactions (that is, don't have GTIDs), and a transaction must be anonymous to be replicated.</p> <p>OFF_PERMISSIVE specifies that new transactions are anonymous transactions, but all transactions can be replicated.</p> <p>ON_PERMISSIVE specifies that new transactions are GTID transactions, but all transactions can be replicated.</p> <p>ON specifies that new transactions are GTID transactions, and a transaction must be a GTID transaction to be replicated.</p>
enforce_gtid_consistency	OFF, ON, WARN	<p>OFF allows transactions to violate GTID consistency.</p> <p>ON prevents transactions from violating GTID consistency.</p> <p>WARN allows transactions to violate GTID consistency but generates a warning when a violation occurs.</p>

Note

In the AWS Management Console, the `gtid_mode` parameter appears as `gtid-mode`.

For GTID-based replication, use these settings for the parameter group for your DB instance or read replica:

- ON and ON_PERMISSIVE apply only to outgoing replication from an RDS DB instance. Both of these values cause your RDS DB instance to use GTIDs for transactions that are replicated. ON requires that the target database also use GTID-based replication. ON_PERMISSIVE makes GTID-based replication optional on the target database.
- OFF_PERMISSIVE, if set, means that your RDS DB instances can accept incoming replication from a source database. They can do this regardless of whether the source database uses GTID-based replication.
- OFF, if set, means that your RDS DB instance only accepts incoming replication from source databases that don't use GTID-based replication.

For more information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

Configuring GTID-based replication for new read replicas

When GTID-based replication is enabled for an RDS for MySQL DB instance, GTID-based replication is configured automatically for read replicas of the DB instance.

To enable GTID-based replication for new read replicas

1. Make sure that the parameter group associated with the DB instance has the following parameter settings:

- `gtid_mode` – ON or ON_PERMISSIVE
- `enforce_gtid_consistency` – ON

For more information about setting configuration parameters using parameter groups, see [Working with parameter groups \(p. 289\)](#).

2. If you changed the parameter group of the DB instance, reboot the DB instance. For more information on how to do so, see [Rebooting a DB instance \(p. 366\)](#).
3. Create one or more read replicas of the DB instance. For more information on how to do so, see [Creating a read replica \(p. 375\)](#).

Amazon RDS attempts to establish GTID-based replication between the MySQL DB instance and the read replicas using the `MASTER_AUTO_POSITION`. If the attempt fails, Amazon RDS uses log file positions for replication with the read replicas. For more information about the `MASTER_AUTO_POSITION`, see [GTID auto-positioning](#) in the MySQL documentation.

Configuring GTID-based replication for existing read replicas

For an existing MySQL DB instance with read replicas that doesn't use GTID-based replication, you can configure GTID-based replication between the DB instance and the read replicas.

To enable GTID-based replication for existing read replicas

1. If the DB instance or any read replica is using an 8.0 version of RDS for MySQL version lower than 8.0.26, upgrade the DB instance or read replica to 8.0.26 or a higher MySQL 8.0 version. All RDS for MySQL 5.7 versions support GTID-based replication.

For more information, see [Upgrading the MySQL DB engine \(p. 1343\)](#).

2. (Optional) Reset the GTID parameters and test the behavior of the DB instance and read replicas:
 - a. Make sure that the parameter group associated with the DB instance and each read replica has the `enforce_gtid_consistency` parameter set to `WARN`.

For more information about setting configuration parameters using parameter groups, see [Working with parameter groups \(p. 289\)](#).
 - b. If you changed the parameter group of the DB instance, reboot the DB instance. If you changed the parameter group for a read replica, reboot the read replica.

For more information, see [Rebooting a DB instance \(p. 366\)](#).
 - c. Run your DB instance and read replicas with your normal workload and monitor the log files.

If you see warnings about GTID-incompatible transactions, adjust your application so that it only uses GTID-compatible features. Make sure that the DB instance is not generating any warnings about GTID-incompatible transactions before proceeding to the next step.

3. Reset the GTID parameters for GTID-based replication that allows anonymous transactions until the read replicas have processed all of them.
 - a. Make sure that the parameter group associated with the DB instance and each read replica has the following parameter settings:
 - `gtid_mode` – `ON_PERMISSIVE`
 - `enforce_gtid_consistency` – ON
 - b. If you changed the parameter group of the DB instance, reboot the DB instance. If you changed the parameter group for a read replica, reboot the read replica.

4. Wait for all of your anonymous transactions to be replicated. To check that these are replicated, do the following:

- a. Run the following statement on your source DB instance.

```
SHOW MASTER STATUS;
```

Note the values in the File and Position columns.

- b. On each read replica, use the file and position information from its source instance in the previous step to run the following query.

```
SELECT MASTER_POS_WAIT('file', position);
```

For example, if the file name is mysql-bin-changelog.000031 and the position is 107, run the following statement.

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

If the read replica is past the specified position, the query returns immediately. Otherwise, the function waits. Proceed to the next step when the query returns for all read replicas.

5. Reset the GTID parameters for GTID-based replication only.

- a. Make sure that the parameter group associated with the DB instance and each read replica has the following parameter settings:

- gtid_mode – ON
- enforce_gtid_consistency – ON

- b. Reboot the DB instance and each read replica.

6. On each read replica, run the following procedure.

```
CALL mysql.rds_set_master_auto_position(1);
```

Disabling GTID-based replication for a MySQL DB instance with read replicas

You can disable GTID-based replication for a MySQL DB instance with read replicas.

To disable GTID-based replication for a MySQL DB instance with read replicas

1. On each read replica, run the following procedure.

```
CALL mysql.rds_set_master_auto_position(0); (Aurora MySQL version 1 and 2)
CALL mysql.rds_set_source_auto_position(0); (Aurora MySQL version 3 and higher)
```

2. Reset the gtid_mode to ON_PERMISSIVE.

- a. Make sure that the parameter group associated with the MySQL DB instance and each read replica has gtid_mode set to ON_PERMISSIVE.

For more information about setting configuration parameters using parameter groups, see [Working with parameter groups \(p. 289\)](#).

- b. Reboot the MySQL DB instance and each read replica. For more information about rebooting, see [Rebooting a DB instance \(p. 366\)](#).
3. Reset the gtid_mode to OFF_PERMISSIVE:
 - a. Make sure that the parameter group associated with the MySQL DB instance and each read replica has gtid_mode set to OFF_PERMISSIVE.
 - b. Reboot the MySQL DB instance and each read replica.
4. Wait for all of the GTID transactions to be applied on all of the read replicas. To check that these are applied, do the following:

Wait for all of the GTID transactions to be applied on the Aurora primary instance. To check that these are applied, do the following:

- a. On the MySQL DB instance, run the SHOW MASTER STATUS command.

Your output should be similar to the following.

File	Position
mysql-bin-changelog.000031	107

Note the file and position in your output.

- b. On each read replica, use the file and position information from its source instance in the previous step to run the following query.

```
SELECT MASTER_POS_WAIT('file', position);
```

For example, if the file name is mysql-bin-changelog.000031 and the position is 107, run the following statement.

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

If the read replica is past the specified position, the query returns immediately. Otherwise, the function waits. When the query returns for all read replicas, go to the next step.

5. Reset the GTID parameters to disable GTID-based replication:
 - a. Make sure that the parameter group associated with the MySQL DB instance and each read replica has the following parameter settings:
 - gtid_mode – OFF
 - enforce_gtid_consistency – OFF
 - b. Reboot the MySQL DB instance and each read replica.

Configuring GTID-based replication with an external source instance

You can set up replication based on global transaction identifiers (GTIDs) from an external MySQL instance into an RDS for MySQL DB instance. When you set up an external source instance and a replica on Amazon RDS, monitor failover events for the Amazon RDS DB instance that is your replica. If a failover occurs, then the DB instance that is your replica might be recreated on a new host with a different

network address. For information on how to monitor failover events, see [Working with Amazon RDS event notification \(p. 650\)](#).

Important

GTID-based replication is supported only on RDS for MySQL version 5.7.23 and higher MySQL 5.7 versions, and RDS for MySQL 8.0.26 and higher 8.0 versions.

To configure GTID-based replication with an external source instance

1. Prepare for GTID-based replication:

- a. Make sure that the external MySQL database has GTID-based replication enabled. To do so, make sure that the external database has the following parameters set to the specified values:

```
gtid_mode - ON
```

```
enforce_gtid_consistency - ON
```

For more information, see [Replication with global transaction identifiers](#) in the MySQL documentation.

- b. Make sure that the parameter group associated with the DB instance has the following parameter settings:
 - gtid_mode - ON, ON_PERMISSIVE, or OFF_PERMISSIVE
 - enforce_gtid_consistency - ON

For more information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

- c. If you changed the parameter group of the DB instance, reboot the DB instance. For more information, see [Rebooting a DB instance \(p. 366\)](#).

2. Make the source MySQL instance read-only.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

3. Copy the database from the external instance to the Amazon RDS DB instance using mysqldump. For very large databases, you might want to use the procedure in [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#).

For Linux, macOS, or Unix:

```
mysqldump --databases database_name \
--single-transaction \
--compress \
--order-by-primary \
-u local_user \
-plocal_password | mysql \
--host=hostname \
--port=3306 \
-u RDS_user_name \
-pRDS_password
```

For Windows:

```
mysqldump --databases database_name ^
--single-transaction ^
--compress ^
--order-by-primary ^
-u local_user ^
```

```
-plocal_password | mysql ^
--host=hostname ^
--port=3306 ^
-u RDS_user_name ^
-pRDS_password
```

Note

Make sure that there isn't a space between the -p option and the entered password.

To specify the host name, user name, port, and password to connect to your Amazon RDS DB instance, use the --host, --user (-u), --port and -p options in the mysql command. The host name is the Domain Name System (DNS) name from the Amazon RDS DB instance endpoint, for example, myinstance.123456789012.us-east-1.rds.amazonaws.com. You can find the endpoint value in the instance details in the AWS Management Console.

4. Make the source MySQL instance writeable again.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

For more information on making backups for use with replication, see [the MySQL documentation](#).

5. On the AWS Management Console, add the IP address of the server that hosts the external database to the virtual private cloud (VPC) security group for the Amazon RDS DB instance. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the [Amazon VPC User Guide](#).

The IP address can change when the following conditions are met:

- You are using a public IP address for communication between the external source instance and the DB instance.
- The external source instance was stopped and restarted.

If these conditions are met, verify the IP address before adding it.

You might also need to configure your local network to permit connections from the IP address of your Amazon RDS DB instance. You do this so that your local network can communicate with your external MySQL instance. To find the IP address of the Amazon RDS DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the Amazon RDS DB instance endpoint.

6. Using the client of your choice, connect to the external instance and create a user to use for replication. Use this account solely for replication. and restrict it to your domain to improve security. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. For the external instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'password';
```

8. Make the Amazon RDS DB instance the replica. To do so, first connect to the Amazon RDS DB instance as the master user. Then identify the external MySQL database as the replication primary instance by using the [mysql.rds_set_external_master_with_auto_position \(p. 1446\)](#) command. The following is an example.

```
CALL mysql.rds_set_external_master_with_auto_position ('mymasterserver.mydomain.com',  
3306, 'repl_user', 'password', 0, 0);
```

Note

On RDS for MySQL, you can choose to use delayed replication by running the [mysql.rds_set_external_master_with_delay \(p. 1443\)](#) stored procedure instead. On RDS for MySQL, one reason to use delayed replication is to enable disaster recovery with the [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure.

9. On the Amazon RDS DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

Configuring binary log file position replication with an external source instance

You can set up replication between an RDS for MySQL or MariaDB DB instance and a MySQL or MariaDB instance that is external to Amazon RDS using binary log file replication.

Topics

- [Before you begin \(p. 1037\)](#)
- [Configuring binary log file position replication with an external source instance \(p. 1037\)](#)

Before you begin

You can configure replication using the binary log file position of replicated transactions.

The permissions required to start replication on an Amazon RDS DB instance are restricted and not available to your Amazon RDS master user. Because of this, make sure that you use the Amazon RDS [mysql.rds_set_external_master \(p. 1441\)](#) and [mysql.rds_start_replication \(p. 1452\)](#) commands to set up replication between your live database and your Amazon RDS database.

To set the binary logging format for a MySQL or MariaDB database, update the `binlog_format` parameter. If your DB instance uses the default DB instance parameter group, create a new DB parameter group to modify `binlog_format` settings. We recommend that you use the default setting for `binlog_format`, which is `MIXED`. However, you can also set `binlog_format` to `ROW` or `STATEMENT` if you need a specific binary log (`binlog`) format. Reboot your DB instance for the change to take effect.

For information about setting the `binlog_format` parameter, see [Configuring MySQL binary logging \(p. 706\)](#). For information about the implications of different MySQL replication types, see [Advantages and disadvantages of statement-based and row-based replication](#) in the MySQL documentation.

Configuring binary log file position replication with an external source instance

Follow these guidelines when you set up an external source instance and a replica on Amazon RDS:

- Monitor failover events for the Amazon RDS DB instance that is your replica. If a failover occurs, then the DB instance that is your replica might be recreated on a new host with a different network address. For information on how to monitor failover events, see [Working with Amazon RDS event notification \(p. 650\)](#).
- Maintain the binlogs on your source instance until you have verified that they have been applied to the replica. This maintenance makes sure that you can restore your source instance in the event of a failure.
- Turn on automated backups on your Amazon RDS DB instance. Turning on automated backups makes sure that you can restore your replica to a particular point in time if you need to re-synchronize your source instance and replica. For information on backups and point-in-time restore, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

To configure binary log file replication with an external source instance

1. Make the source MySQL or MariaDB instance read-only.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Run the SHOW MASTER STATUS command on the source MySQL or MariaDB instance to determine the binlog location.

You receive output similar to the following example.

File	Position
mysql-bin-changelog.000031	107

3. Copy the database from the external instance to the Amazon RDS DB instance using mysqldump. For very large databases, you might want to use the procedure in [Importing data to an Amazon RDS MariaDB or MySQL DB instance with reduced downtime \(p. 1371\)](#).

For Linux, macOS, or Unix:

```
mysqldump --databases database_name \
    --single-transaction \
    --compress \
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql \
    --host=hostname \
    --port=3306 \
    -u RDS_user_name \
    -pRDS_password
```

For Windows:

```
mysqldump --databases database_name ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    -u local_user ^
    -plocal_password | mysql ^
    --host=hostname ^
    --port=3306 ^
    -u RDS_user_name ^
    -pRDS_password
```

Note

Make sure that there isn't a space between the -p option and the entered password.

To specify the host name, user name, port, and password to connect to your Amazon RDS DB instance, use the --host, --user (-u), --port and -p options in the mysql command. The host name is the Domain Name Service (DNS) name from the Amazon RDS DB instance endpoint, for example myinstance.123456789012.us-east-1.rds.amazonaws.com. You can find the endpoint value in the instance details in the AWS Management Console.

4. Make the source MySQL or MariaDB instance writeable again.

```
mysql> SET GLOBAL read_only = OFF;  
mysql> UNLOCK TABLES;
```

For more information on making backups for use with replication, see [the MySQL documentation](#).

5. In the AWS Management Console, add the IP address of the server that hosts the external database to the virtual private cloud (VPC) security group for the Amazon RDS DB instance. For more information on modifying a VPC security group, see [Security groups for your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.

The IP address can change when the following conditions are met:

- You are using a public IP address for communication between the external source instance and the DB instance.
- The external source instance was stopped and restarted.

If these conditions are met, verify the IP address before adding it.

You might also need to configure your local network to permit connections from the IP address of your Amazon RDS DB instance. You do this so that your local network can communicate with your external MySQL or MariaDB instance. To find the IP address of the Amazon RDS DB instance, use the host command.

```
host db_instance_endpoint
```

The host name is the DNS name from the Amazon RDS DB instance endpoint.

6. Using the client of your choice, connect to the external instance and create a user to use for replication. Use this account solely for replication and restrict it to your domain to improve security. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

7. For the external instance, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. For example, to grant the REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the 'repl_user' user for your domain, issue the following command.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Make the Amazon RDS DB instance the replica. To do so, first connect to the Amazon RDS DB instance as the master user. Then identify the external MySQL or MariaDB database as the source instance by using the [mysql.rds_set_external_master \(p. 1441\)](#) command. Use the master log file name and master log position that you determined in step 2. The following is an example.

```
CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306, 'repl_user',  
'password', 'mysql-bin-changelog.000031', 107, 0);
```

Note

On RDS for MySQL, you can choose to use delayed replication by running the [mysql.rds_set_external_master_with_delay \(p. 1443\)](#) stored procedure instead.

On RDS for MySQL, one reason to use delayed replication is to turn on disaster

recovery with the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure.

Currently, RDS for MariaDB supports delayed replication but doesn't support the [mysql.rds_start_replication_until](#) procedure.

9. On the Amazon RDS DB instance, issue the [mysql.rds_start_replication \(p. 1452\)](#) command to start replication.

```
CALL mysql.rds_start_replication;
```

Exporting data from a MySQL DB instance by using replication

To export data from an RDS for MySQL DB instance to a MySQL instance running external to Amazon RDS, you can use replication. In this scenario, the MySQL DB instance is the *source MySQL DB instance*, and the MySQL instance running external to Amazon RDS is the *external MySQL database*.

The external MySQL database can run either on-premises in your data center, or on an Amazon EC2 instance. The external MySQL database must run the same version as the source MySQL DB instance, or a later version.

Replication to an external MySQL database is only supported during the time it takes to export a database from the source MySQL DB instance. The replication should be terminated when the data has been exported and applications can start accessing the external MySQL instance.

The following list shows the steps to take. Each step is discussed in more detail in later sections.

1. Prepare an external MySQL DB instance.
2. Prepare the source MySQL DB instance for replication.
3. Use the mysqldump utility to transfer the database from the source MySQL DB instance to the external MySQL database.
4. Start replication to the external MySQL database.
5. After the export completes, stop replication.

Prepare an external MySQL database

Perform the following steps to prepare the external MySQL database.

To prepare the external MySQL database

1. Install the external MySQL database.
2. Connect to the external MySQL database as the master user. Then create the users required to support the administrators, applications, and services that access the database.
3. Follow the directions in the MySQL documentation to prepare the external MySQL database as a replica. For more information, see [the MySQL documentation](#).
4. Configure an egress rule for the external MySQL database to operate as a read replica during the export. The egress rule allows the external MySQL database to connect to the source MySQL DB instance during replication. Specify an egress rule that allows Transmission Control Protocol (TCP) connections to the port and IP address of the source MySQL DB instance.

Specify the appropriate egress rules for your environment:

- If the external MySQL database is running in an Amazon EC2 instance in a virtual private cloud (VPC) based on the Amazon VPC service, specify the egress rules in a VPC security group. For more information, see [Controlling access with security groups \(p. 2085\)](#).
 - If the external MySQL database is installed on-premises, specify the egress rules in a firewall.
5. If the external MySQL database is running in a VPC, configure rules for the VPC access control list (ACL) rules in addition to the security group egress rule:
 - Configure an ACL ingress rule allowing TCP traffic to ports 1024–65535 from the IP address of the source MySQL DB instance.
 - Configure an ACL egress rule allowing outbound TCP traffic to the port and IP address of the source MySQL DB instance.

For more information about Amazon VPC network ACLs, see [Network ACLs](#) in *Amazon VPC User Guide*.

6. (Optional) Set the `max_allowed_packet` parameter to the maximum size to avoid replication errors. We recommend this setting.

Prepare the source MySQL DB instance

Perform the following steps to prepare the source MySQL DB instance as the replication source.

To prepare the source MySQL DB instance

1. Ensure that your client computer has enough disk space available to save the binary logs while setting up replication.
2. Connect to the source MySQL DB instance, and create a replication account by following the directions in [Creating a user for replication](#) in the MySQL documentation.
3. Configure ingress rules on the system running the source MySQL DB instance to allow the external MySQL database to connect during replication. Specify an ingress rule that allows TCP connections to the port used by the source MySQL DB instance from the IP address of the external MySQL database.
4. Specify the egress rules:
 - If the source MySQL DB instance is running in a VPC, specify the ingress rules in a VPC security group. For more information, see [Controlling access with security groups \(p. 2085\)](#).
5. If source MySQL DB instance is running in a VPC, configure VPC ACL rules in addition to the security group ingress rule:
 - Configure an ACL ingress rule to allow TCP connections to the port used by the Amazon RDS instance from the IP address of the external MySQL database.
 - Configure an ACL egress rule to allow TCP connections from ports 1024–65535 to the IP address of the external MySQL database.

For more information about Amazon VPC network ACLs, see [Network ACLs](#) in the *Amazon VPC User Guide*.

6. Ensure that the backup retention period is set long enough that no binary logs are purged during the export. If any of the logs are purged before the export has completed, you must restart replication from the beginning. For more information about setting the backup retention period, see [Working with backups \(p. 427\)](#).
7. Use the `mysql.rds_set_configuration` stored procedure to set the binary log retention period long enough that the binary logs aren't purged during the export. For more information, see [Accessing MySQL binary logs \(p. 707\)](#).
8. Create an Amazon RDS read replica from the source MySQL DB instance to further ensure that the binary logs of the source MySQL DB instance are not purged. For more information, see [Creating a read replica \(p. 375\)](#).
9. After the Amazon RDS read replica has been created, call the `mysql.rds_stop_replication` stored procedure to stop the replication process. The source MySQL DB instance no longer purges its binary log files, so they are available for the replication process.
10. (Optional) Set both the `max_allowed_packet` parameter and the `slave_max_allowed_packet` parameter to the maximum size to avoid replication errors. The maximum size for both parameters is 1 GB. We recommend this setting for both parameters. For information about setting parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Copy the database

Perform the following steps to copy the database.

To copy the database

1. Connect to the RDS read replica of the source MySQL DB instance, and run the MySQL SHOW REPLICA STATUS\G statement. Note the values for the following:

- Master_Host
- Master_Port
- Master_Log_File
- Exec_Master_Log_Pos

Note

Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

2. Use the mysqldump utility to create a snapshot, which copies the data from Amazon RDS to your local client computer. Ensure that your client computer has enough space to hold the mysqldump files from the databases to be replicated. This process can take several hours for very large databases. Follow the directions in [Creating a data snapshot using mysqldump](#) in the MySQL documentation.

The following example runs mysqldump on a client and writes the dump to a file.

For Linux, macOS, or Unix:

```
mysqldump -h source_MySQL_DB_instance_endpoint \
-u user \
-ppassword \
--port=3306 \
--single-transaction \
--routines \
--triggers \
--databases database database2 > path/rds-dump.sql
```

For Windows:

```
mysqldump -h source_MySQL_DB_instance_endpoint ^
-u user ^
-ppassword ^
--port=3306 ^
--single-transaction ^
--routines ^
--triggers ^
--databases database database2 > path\rds-dump.sql
```

You can load the backup file into the external MySQL database. For more information, see [Reloading SQL-Format Backups](#) in the MySQL documentation. You can run another utility to load the data into the external MySQL database.

Complete the export

Perform the following steps to complete the export.

To complete the export

1. Use the MySQL CHANGE MASTER statement to configure the external MySQL database. Specify the ID and password of the user granted REPLICATION SLAVE permissions. Specify the Master_Host, Master_Port, Relay_Master_Log_File, and Exec_Master_Log_Pos values that you got from the MySQL SHOW REPLICA STATUS\G statement that you ran on the RDS read replica. For more information, see [the MySQL documentation](#).

Note

Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

2. Use the MySQL START REPLICA command to initiate replication from the source MySQL DB instance to the external MySQL database.

Doing this starts replication from the source MySQL DB instance and exports all source changes that have occurred after you stopped replication from the Amazon RDS read replica.

Note

Previous versions of MySQL used START SLAVE instead of START REPLICA. If you are using a MySQL version before 8.0.23, then use START SLAVE.

3. Run the MySQL SHOW REPLICA STATUS\G command on the external MySQL database to verify that it is operating as a read replica. For more information about interpreting the results, see [the MySQL documentation](#).
4. After replication on the external MySQL database has caught up with the source MySQL DB instance, use the MySQL STOP REPLICA command to stop replication from the source MySQL DB instance.

Note

Previous versions of MySQL used STOP SLAVE instead of STOP REPLICA. If you are using a MySQL version before 8.0.23, then use STOP SLAVE.

5. On the Amazon RDS read replica, call the mysql.rds_start_replication stored procedure. Doing this allows Amazon RDS to start purging the binary log files from the source MySQL DB instance.

Options for MySQL DB instances

Following, you can find a description of options, or additional features, that are available for Amazon RDS instances running the MySQL DB engine. To enable these options, you can add them to a custom option group, and then associate the option group with your DB instance. For more information about working with option groups, see [Working with option groups \(p. 273\)](#).

Amazon RDS supports the following options for MySQL:

Option	Option ID	Engine versions
MariaDB Audit Plugin support (p. 1417)	MARIADB_AUDIT_PLUGIN	MySQL 8.0.25 and higher 8.0 versions All MySQL 5.7 versions
MySQL memcached support (p. 1422)	MEMCACHED	All MySQL 5.7 and 8.0 versions

MariaDB Audit Plugin support

Amazon RDS supports using the MariaDB Audit Plugin on MySQL database instances. The MariaDB Audit Plugin records database activity such as users logging on to the database, queries run against the database, and more. The record of database activity is stored in a log file.

Note

Currently, the MariaDB Audit Plugin is only supported for the following RDS for MySQL versions:

- MySQL 8.0.25 and higher 8.0 versions
- All MySQL 5.7 versions

An open source version of this plugin is available, so that you can use it with any MySQL database. For more information, see the [Audit Plugin for MySQL Server GitHub repository](#).

Audit Plugin option settings

Amazon RDS supports the following settings for the MariaDB Audit Plugin option.

Option setting	Valid values	Default value	Description
SERVER_AUDIT_FILEDATA/log/audit/	/rdsdbdata/log/audit/	/rdsdbdata/log/audit/	The location of the log file. The log file contains the record of the activity specified in SERVER_AUDIT_EVENTS. For more information, see Viewing and listing database log files (p. 680) and MySQL database log files (p. 700) .
SERVER_AUDIT_FILEROTATIONSIZE	100000		The size in bytes that when reached, causes the file to rotate. For more information, see Overview of RDS for MySQL database logs (p. 700) .
SERVER_AUDIT_FILEROTATIONS	9		The number of log rotations to save. For more information, see Overview of RDS for MySQL database logs (p. 700) and Downloading a database log file (p. 681) .
SERVER_AUDIT_EVENTS	CONNECT, QUERY, QUERY_DDL, QUERY_DML, QUERY_DML_NO_SELECT, QUERY_DCL	CONNECT, QUERY	<p>The types of activity to record in the log. Installing the MariaDB Audit Plugin is itself logged.</p> <ul style="list-style-type: none">• CONNECT: Log successful and unsuccessful connections to the database, and disconnections from the database.• QUERY: Log the text of all queries run against the database.• QUERY_DDL: Similar to the QUERY event, but returns only data definition language (DDL) queries (CREATE, ALTER, and so on).• QUERY_DML: Similar to the QUERY event, but returns only data manipulation language (DML) queries (INSERT, UPDATE, and so on, and also SELECT).• QUERY_DML_NO_SELECT: Similar to the QUERY_DML event, but doesn't log SELECT queries.

Option setting	Valid values	Default value	Description
			<p>The QUERY_DML_NO_SELECT setting is supported only for RDS for MySQL 5.7.34 and higher 5.7 versions, and 8.0.25 and higher 8.0 versions.</p> <ul style="list-style-type: none"> • QUERY_DCL: Similar to the QUERY event, but returns only data control language (DCL) queries (GRANT, REVOKE, and so on). <p>For MySQL, TABLE is not supported.</p>
SERVER_AUDIT_INCL_USERS	Multiples comma-separated values	None	<p>Include only activity from the specified users. By default, activity is recorded for all users. SERVER_AUDIT_INCL_USERS and SERVER_AUDIT_EXCL_USERS are mutually exclusive. If you add values to SERVER_AUDIT_INCL_USERS, make sure no values are added to SERVER_AUDIT_EXCL_USERS.</p>
SERVER_AUDIT_EXCL_USERS	Multiples comma-separated values	None	<p>Exclude activity from the specified users. By default, activity is recorded for all users. SERVER_AUDIT_INCL_USERS and SERVER_AUDIT_EXCL_USERS are mutually exclusive. If you add values to SERVER_AUDIT_EXCL_USERS, make sure no values are added to SERVER_AUDIT_INCL_USERS.</p> <p>The rdsadmin user queries the database every second to check the health of the database. Depending on your other settings, this activity can possibly cause the size of your log file to grow very large, very quickly. If you don't need to record this activity, add the rdsadmin user to the SERVER_AUDIT_EXCL_USERS list.</p> <p>Note CONNECT activity is always recorded for all users, even if the user is specified for this option setting.</p>
SERVER_AUDIT_LOGGING	ON	ON	<p>Logging is active. The only valid value is ON. Amazon RDS does not support deactivating logging. If you want to deactivate logging, remove the MariaDB Audit Plugin. For more information, see Removing the MariaDB Audit Plugin (p. 1420).</p>
SERVER_AUDIT_QUERYLIMIT	1024		<p>The limit on the length of the query string in a record.</p>

Adding the MariaDB Audit Plugin

The general process for adding the MariaDB Audit Plugin to a DB instance is the following:

- Create a new option group, or copy or modify an existing option group
- Add the option to the option group
- Associate the option group with the DB instance

After you add the MariaDB Audit Plugin, you don't need to restart your DB instance. As soon as the option group is active, auditing begins immediately.

Important

Adding the MariaDB Audit Plugin to a DB instance might cause an outage. We recommend adding the MariaDB Audit Plugin during a maintenance window or during a time of low database workload.

To add the MariaDB Audit Plugin

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group. Choose **mysql** for **Engine**, and choose **5.7** or **8.0** for **Major engine version**. For more information, see [Creating an option group \(p. 274\)](#).
2. Add the **MARIADB_AUDIT_PLUGIN** option to the option group, and configure the option settings. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#). For more information about each setting, see [Audit Plugin option settings \(p. 1417\)](#).
3. Apply the option group to a new or existing DB instance.
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Audit log format

Log files are represented as comma-separated variable (CSV) files in UTF-8 format. The audit log is stored separately on the local (ephemeral) storage of each RDS for MySQL DB instance.

Tip

Log file entries are not in sequential order. To order the entries, use the timestamp value. To see the latest events, you might have to review all log files. For more flexibility in sorting and searching the log data, turn on the setting to upload the audit logs to CloudWatch and view them using the CloudWatch interface.

To view audit data with more types of fields and with output in JSON format, you can also use the Database Activity Streams feature. For more information, see [Monitoring Amazon RDS for Oracle with Database Activity Streams \(p. 729\)](#).

The audit log files include the following comma-delimited information in rows, in the specified order:

Field	Description
timestamp	The Unix time stamp for the logged event with microsecond precision.
serverhost	The name of the instance that the event is logged for.
username	The connected user name of the user.
host	The host that the user connected from.
connectionid	The connection ID number for the logged operation.

Field	Description
queryid	The query ID number, which can be used for finding the relational table events and related queries. For TABLE events, multiple lines are added.
operation	The recorded action type. Possible values are: CONNECT, QUERY, READ, WRITE, CREATE, ALTER, RENAME, and DROP.
database	The active database, as set by the USE command.
object	For QUERY events, this value indicates the query that the database performed. For TABLE events, it indicates the table name.
retcode	The return code of the logged operation.
connection_type	<p>The security state of the connection to the server. Possible values are:</p> <ul style="list-style-type: none"> • 0 – Undefined • 1 – TCP/IP • 2 – Socket • 3 – Named pipe • 4 – SSL/TLS • 5 – Shared memory <p>This field is included only for RDS for MySQL version 5.7.34 and higher 5.7 versions, and all 8.0 versions.</p>

Viewing and downloading the MariaDB Audit Plugin log

After you enable the MariaDB Audit Plugin, you access the results in the log files the same way you access any other text-based log files. The audit log files are located at `/rdsdbdata/log/audit/`. For information about viewing the log file in the console, see [Viewing and listing database log files \(p. 680\)](#). For information about downloading the log file, see [Downloading a database log file \(p. 681\)](#).

Modifying MariaDB Audit Plugin settings

After you enable the MariaDB Audit Plugin, you can modify the settings. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [Audit Plugin option settings \(p. 1417\)](#).

Removing the MariaDB Audit Plugin

Amazon RDS doesn't support turning off logging in the MariaDB Audit Plugin. However, you can remove the plugin from a DB instance. When you remove the MariaDB Audit Plugin, the DB instance is restarted automatically to stop auditing.

To remove the MariaDB Audit Plugin from a DB instance, do one of the following:

- Remove the MariaDB Audit Plugin option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#)
- Modify the DB instance and specify a different option group that doesn't include the plugin. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

MySQL memcached support

Amazon RDS supports using the memcached interface to InnoDB tables that was introduced in MySQL 5.6. The memcached API enables applications to use InnoDB tables in a manner similar to NoSQL key-value data stores.

The memcached interface is a simple, key-based cache. Applications use memcached to insert, manipulate, and retrieve key-value data pairs from the cache. MySQL 5.6 introduced a plugin that implements a daemon service that exposes data from InnoDB tables through the memcached protocol. For more information about the MySQL memcached plugin, see [InnoDB integration with memcached](#).

To enable memcached support for an RDS for MySQL DB instance

1. Determine the security group to use for controlling access to the memcached interface. If the set of applications already using the SQL interface are the same set that will access the memcached interface, you can use the existing VPC security group used by the SQL interface. If a different set of applications will access the memcached interface, define a new VPC or DB security group. For more information about managing security groups, see [Controlling access with security groups \(p. 2085\)](#)
2. Create a custom DB option group, selecting MySQL as the engine type and version. For more information about creating an option group, see [Creating an option group \(p. 274\)](#).
3. Add the MEMCACHED option to the option group. Specify the port that the memcached interface will use, and the security group to use in controlling access to the interface. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
4. Modify the option settings to configure the memcached parameters, if necessary. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#).
5. Apply the option group to an instance. Amazon RDS enables memcached support for that instance when the option group is applied:
 - You enable memcached support for a new instance by specifying the custom option group when you launch the instance. For more information about launching a MySQL instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - You enable memcached support for an existing instance by specifying the custom option group when you modify the instance. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
6. Specify which columns in your MySQL tables can be accessed through the memcached interface. The memcached plug-in creates a catalog table named `containers` in a dedicated database named `innodb_memcache`. You insert a row into the `containers` table to map an InnoDB table for access through memcached. You specify a column in the InnoDB table that is used to store the memcached key values, and one or more columns that are used to store the data values associated with the key. You also specify a name that a memcached application uses to refer to that set of columns. For details on inserting rows in the `containers` table, see [InnoDB memcached plugin internals](#). For an example of mapping an InnoDB table and accessing it through memcached, see [Writing applications for the InnoDB memcached plugin](#).
7. If the applications accessing the memcached interface are on different computers or EC2 instances than the applications using the SQL interface, add the connection information for those computers to the VPC security group associated with the MySQL instance. For more information about managing security groups, see [Controlling access with security groups \(p. 2085\)](#).

You turn off the memcached support for an instance by modifying the instance and specifying the default option group for your MySQL version. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

MySQL memcached security considerations

The memcached protocol does not support user authentication. For more information about MySQL memcached security considerations, see [memcached deployment](#) and [Using memcached as a MySQL caching layer](#).

You can take the following actions to help increase the security of the memcached interface:

- Specify a different port than the default of 11211 when adding the MEMCACHED option to the option group.
- Ensure that you associate the memcached interface with a VPC security group that limits access to known, trusted client addresses and EC2 instances. For more information about managing security groups, see [Controlling access with security groups \(p. 2085\)](#).

MySQL memcached connection information

To access the memcached interface, an application must specify both the DNS name of the Amazon RDS instance and the memcached port number. For example, if an instance has a DNS name of my-cache-instance.cg034hpkmjt.region.rds.amazonaws.com and the memcached interface is using port 11212, the connection information specified in PHP would be:

```
<?php  
  
$cache = new Memcache;  
$cache->connect('my-cache-instance.cg034hpkmjt.region.rds.amazonaws.com', 11212);  
?>
```

To find the DNS name and memcached port of a MySQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top right corner of the AWS Management Console, select the region that contains the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose the MySQL DB instance name to display its details.
5. In the **Connect** section, note the value of the **Endpoint** field. The DNS name is the same as the endpoint. Also, note that the port in the **Connect** section is not used to access the memcached interface.
6. In the **Details** section, note the name listed in the **Option Group** field.
7. In the navigation pane, choose **Option groups**.
8. Choose the name of the option group used by the MySQL DB instance to show the option group details. In the **Options** section, note the value of the **Port** setting for the **MEMCACHED** option.

MySQL memcached option settings

Amazon RDS exposes the MySQL memcached parameters as option settings in the Amazon RDS MEMCACHED option.

MySQL memcached parameters

- DAEMON_MEMCACHED_R_BATCH_SIZE – an integer that specifies how many memcached read operations (get) to perform before doing a COMMIT to start a new transaction. The allowed values are 1 to 4294967295; the default is 1. The option does not take effect until the instance is restarted.

- DAEMON_MEMCACHED_W_BATCH_SIZE – an integer that specifies how many memcached write operations, such as add, set, or incr, to perform before doing a COMMIT to start a new transaction. The allowed values are 1 to 4294967295; the default is 1. The option does not take effect until the instance is restarted.
- INNODB_API_BK_COMMIT_INTERVAL – an integer that specifies how often to auto-commit idle connections that use the InnoDB memcached interface. The allowed values are 1 to 1073741824; the default is 5. The option takes effect immediately, without requiring that you restart the instance.
- INNODB_API_DISABLE_ROWLOCK – a Boolean that disables (1 (true)) or enables (0 (false)) the use of row locks when using the InnoDB memcached interface. The default is 0 (false). The option does not take effect until the instance is restarted.
- INNODB_API_ENABLE_MDL – a Boolean that when set to 0 (false) locks the table used by the InnoDB memcached plugin, so that it cannot be dropped or altered by DDL through the SQL interface. The default is 0 (false). The option does not take effect until the instance is restarted.
- INNODB_API_TRX_LEVEL – an integer that specifies the transaction isolation level for queries processed by the memcached interface. The allowed values are 0 to 3. The default is 0. The option does not take effect until the instance is restarted.

Amazon RDS configures these MySQL memcached parameters, and they cannot be modified: DAEMON_MEMCACHED_LIB_NAME, DAEMON_MEMCACHED_LIB_PATH, and INNODB_API_ENABLE_BINLOG. The parameters that MySQL administrators set by using `daemon_memcached_options` are available as individual MEMCACHED option settings in Amazon RDS.

MySQL `daemon_memcached_options` parameters

- BINDING_PROTOCOL – a string that specifies the binding protocol to use. The allowed values are auto, ascii, or binary. The default is auto, which means the server automatically negotiates the protocol with the client. The option does not take effect until the instance is restarted.
- BACKLOG_QUEUE_LIMIT – an integer that specifies how many network connections can be waiting to be processed by memcached. Increasing this limit may reduce errors received by a client that is not able to connect to the memcached instance, but does not improve the performance of the server. The allowed values are 1 to 2048; the default is 1024. The option does not take effect until the instance is restarted.
- CAS_DISABLED – a Boolean that enables (1 (true)) or disables (0 (false)) the use of compare and swap (CAS), which reduces the per-item size by 8 bytes. The default is 0 (false). The option does not take effect until the instance is restarted.
- CHUNK_SIZE – an integer that specifies the minimum chunk size, in bytes, to allocate for the smallest item's key, value, and flags. The allowed values are 1 to 48. The default is 48 and you can significantly improve memory efficiency with a lower value. The option does not take effect until the instance is restarted.
- CHUNK_SIZE_GROWTH_FACTOR – a float that controls the size of new chunks. The size of a new chunk is the size of the previous chunk times CHUNK_SIZE_GROWTH_FACTOR. The allowed values are 1 to 2; the default is 1.25. The option does not take effect until the instance is restarted.
- ERROR_ON_MEMORY_EXHAUSTED – a Boolean that when set to 1 (true) specifies that memcached will return an error rather than evicting items when there is no more memory to store items. If set to 0 (false), memcached will evict items if there is no more memory. The default is 0 (false). The option does not take effect until the instance is restarted.
- MAX_SIMULTANEOUS_CONNECTIONS – an integer that specifies the maximum number of concurrent connections. Setting this value to anything under 10 prevents MySQL from starting. The allowed values are 10 to 1024; the default is 1024. The option does not take effect until the instance is restarted.
- VERTBOSITY – a string that specifies the level of information logged in the MySQL error log by the memcached service. The default is v. The option does not take effect until the instance is restarted. The allowed values are:

- v – Logs errors and warnings while running the main event loop.
- vv – In addition to the information logged by v, also logs each client command and the response.
- vvv – In addition to the information logged by vv, also logs internal state transitions.

Amazon RDS configures these MySQL DAEMON_MEMCACHED_OPTIONS parameters, they cannot be modified: DAEMON_PROCESS, LARGE_MEMORY_PAGES, MAXIMUM_CORE_FILE_LIMIT, MAX_ITEM_SIZE, LOCK_DOWN_PAGE_MEMORY, MASK, IDFILE, REQUESTS_PER_EVENT, SOCKET, and USER.

Parameters for MySQL

By default, a MySQL DB instance uses a DB parameter group that is specific to a MySQL database. This parameter group contains parameters for the MySQL database engine. For information about working with parameter groups and setting parameters, see [Working with parameter groups \(p. 289\)](#).

RDS for MySQL parameters are set to the default values of the storage engine that you have selected. For more information about MySQL parameters, see the [MySQL documentation](#). For more information about MySQL storage engines, see [Supported storage engines for RDS for MySQL \(p. 1312\)](#).

You can view the parameters available for a specific RDS for MySQL version using the RDS console or the AWS CLI. For information about viewing the parameters in a MySQL parameter group in the RDS console, see [Viewing parameter values for a DB parameter group \(p. 301\)](#).

Using the AWS CLI, you can view the parameters for an RDS for MySQL version by running the `describe-engine-default-parameters` command. Specify one of the following values for the `--db-parameter-group-family` option:

- mysql8.0
- mysql5.7

For example, to view the parameters for RDS for MySQL version 8.0, run the following command.

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0
```

Your output looks similar to the following.

```
{  
    "EngineDefaults": {  
        "Parameters": [  
            {  
                "ParameterName": "activate_all_roles_on_login",  
                "ParameterValue": "0",  
                "Description": "Automatically set all granted roles as active after the user has authenticated successfully.",  
                "Source": "engine-default",  
                "ApplyType": "dynamic",  
                "DataType": "boolean",  
                "AllowedValues": "0,1",  
                "IsModifiable": true  
            },  
            {  
                "ParameterName": "allow-suspicious-udfs",  
                "Description": "Controls whether user-defined functions that have only an xxx symbol for the main function can be loaded",  
                "Source": "engine-default",  
                "ApplyType": "static",  
                "DataType": "boolean",  
                "AllowedValues": "0,1",  
                "IsModifiable": false  
            },  
            {  
                "ParameterName": "auto_generate_certs",  
                "Description": "Controls whether the server autogenerates SSL key and certificate files in the data directory, if they do not already exist.",  
                "Source": "engine-default",  
                "ApplyType": "static",  
                "DataType": "boolean",  
                "AllowedValues": "0,1",  
                "IsModifiable": true  
            }  
        ]  
    }  
}
```

```
        "IsModifiable": false
    },
    ...
}
```

To list only the modifiable parameters for RDS for MySQL version 8.0, run the following command.

For Linux, macOS, or Unix:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0 \
--query 'EngineDefaults.Parameters[?IsModifiable==`true`]'
```

For Windows:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0 ^
--query "EngineDefaults.Parameters[?IsModifiable==`true`]"
```

Common DBA tasks for MySQL DB instances

Following, you can find descriptions of the Amazon RDS–specific implementations of some common DBA tasks for DB instances running the MySQL database engine. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. Also, it restricts access to certain system procedures and tables that require advanced privileges.

For information about working with MySQL log files on Amazon RDS, see [MySQL database log files \(p. 700\)](#).

Topics

- [Ending a session or query \(p. 1428\)](#)
- [Skipping the current replication error \(p. 1428\)](#)
- [Working with InnoDB tablespaces to improve crash recovery times \(p. 1429\)](#)
- [Managing the global status history \(p. 1431\)](#)

Ending a session or query

You can end user sessions or queries on DB instances by using the `rds_kill` and `rds_kill_query` commands. First connect to your MySQL DB instance, then issue the appropriate command as shown following. For more information, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#).

```
CALL mysql.rds_kill(thread-ID)
CALL mysql.rds_kill_query(thread-ID)
```

For example, to end the session that is running on thread 99, you would type the following:

```
CALL mysql.rds_kill(99);
```

To end the query that is running on thread 99, you would type the following:

```
CALL mysql.rds_kill_query(99);
```

Skipping the current replication error

You can skip an error on your read replica if the error is causing your read replica to stop responding and the error doesn't affect the integrity of your data.

Note

First verify that the error in question can be safely skipped. In a MySQL utility, connect to the read replica and run the following MySQL command.

```
SHOW REPLICAS STATUS\G
```

For information about the values returned, see [the MySQL documentation](#).

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICAS STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

You can skip an error on your read replica in the following ways.

Topics

- [Calling the mysql.rds_skip_repl_error procedure \(p. 1429\)](#)
- [Setting the slave_skip_errors parameter \(p. 1429\)](#)

Calling the mysql.rds_skip_repl_error procedure

Amazon RDS provides a stored procedure that you can call to skip an error on your read replicas. First connect to your read replica, then issue the appropriate commands as shown following. For more information, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#).

To skip the error, issue the following command.

```
CALL mysql.rds_skip_repl_error;
```

This command has no effect if you run it on the source DB instance, or on a read replica that hasn't encountered a replication error.

For more information, such as the versions of MySQL that support `mysql.rds_skip_repl_error`, see [mysql.rds_skip_repl_error \(p. 1455\)](#).

Important

If you attempt to call `mysql.rds_skip_repl_error` and encounter the following error:
`ERROR 1305 (42000): PROCEDURE mysql.rds_skip_repl_error does not exist`,
then upgrade your MySQL DB instance to the latest minor version or one of the minimum minor versions listed in [mysql.rds_skip_repl_error \(p. 1455\)](#).

Setting the slave_skip_errors parameter

To skip one or more errors, you can set the `slave_skip_errors` static parameter on the read replica. You can set this parameter to skip one or more specific replication error codes. Currently, you can set this parameter only for RDS for MySQL 5.7 DB instances. After you change the setting for this parameter, make sure to reboot your DB instance for the new setting to take effect. For information about setting this parameter, see the [MySQL documentation](#).

We recommend setting this parameter in a separate DB parameter group. You can associate this DB parameter group only with the read replicas that need to skip errors. Following this best practice reduces the potential impact on other DB instances and read replicas.

Important

Setting a nondefault value for this parameter can lead to replication inconsistency. Only set this parameter to a nondefault value if you have exhausted other options to resolve the problem and you are sure of the potential impact on your read replica's data.

Working with InnoDB tablespaces to improve crash recovery times

Every table in MySQL consists of a table definition, data, and indexes. The MySQL storage engine InnoDB stores table data and indexes in a *tablespace*. InnoDB creates a global shared tablespace that contains a data dictionary and other relevant metadata, and it can contain table data and indexes. InnoDB can also create separate tablespaces for each table and partition. These separate tablespaces are stored in files with a .ibd extension and the header of each tablespace contains a number that uniquely identifies it.

Amazon RDS provides a parameter in a MySQL parameter group called `innodb_file_per_table`. This parameter controls whether InnoDB adds new table data and indexes to the shared tablespace (by setting the parameter value to 0) or to individual tablespaces (by setting the parameter value to 1). Amazon RDS sets the default value for `innodb_file_per_table` parameter to 1, which allows you to

drop individual InnoDB tables and reclaim storage used by those tables for the DB instance. In most use cases, setting the `innodb_file_per_table` parameter to 1 is the recommended setting.

You should set the `innodb_file_per_table` parameter to 0 when you have a large number of tables, such as over 1000 tables when you use standard (magnetic) or general purpose SSD storage or over 10,000 tables when you use Provisioned IOPS storage. When you set this parameter to 0, individual tablespaces are not created and this can improve the time it takes for database crash recovery.

MySQL processes each metadata file, which includes tablespaces, during the crash recovery cycle. The time it takes MySQL to process the metadata information in the shared tablespace is negligible compared to the time it takes to process thousands of tablespace files when there are multiple tablespaces. Because the tablespace number is stored within the header of each file, the aggregate time to read all the tablespace files can take up to several hours. For example, a million InnoDB tablespaces on standard storage can take from five to eight hours to process during a crash recovery cycle. In some cases, InnoDB can determine that it needs additional cleanup after a crash recovery cycle so it will begin another crash recovery cycle, which will extend the recovery time. Keep in mind that a crash recovery cycle also entails rolling-back transactions, fixing broken pages, and other operations in addition to the processing of tablespace information.

Since the `innodb_file_per_table` parameter resides in a parameter group, you can change the parameter value by editing the parameter group used by your DB instance without having to reboot the DB instance. After the setting is changed, for example, from 1 (create individual tables) to 0 (use shared tablespace), new InnoDB tables will be added to the shared tablespace while existing tables continue to have individual tablespaces. To move an InnoDB table to the shared tablespace, you must use the `ALTER TABLE` command.

Migrating multiple tablespaces to the shared tablespace

You can move an InnoDB table's metadata from its own tablespace to the shared tablespace, which will rebuild the table metadata according to the `innodb_file_per_table` parameter setting. First connect to your MySQL DB instance, then issue the appropriate commands as shown following. For more information, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#).

```
ALTER TABLE table_name ENGINE = InnoDB, ALGORITHM=COPY;
```

For example, the following query returns an `ALTER TABLE` statement for every InnoDB table that is not in the shared tablespace.

For MySQL 5.7 DB instances:

```
SELECT CONCAT('ALTER TABLE `',
REPLACE(LEFT(NAME , INSTR((NAME), '/') - 1), '`', '''), ``,
REPLACE(SUBSTR(NAME FROM INSTR(NAME, '/') + 1), '`', '''), ``,
ENGINE=InnoDB,
ALGORITHM=COPY;') AS Query
FROM INFORMATION_SCHEMA.INNODB_SYS_TABLES
WHERE SPACE <> 0 AND LEFT(NAME, INSTR((NAME), '/') - 1) NOT IN ('mysql','');
```

For MySQL 8.0 DB instances:

```
SELECT CONCAT('ALTER TABLE `',
REPLACE(LEFT(NAME , INSTR((NAME), '/') - 1), '`', '''), ``,
REPLACE(SUBSTR(NAME FROM INSTR(NAME, '/') + 1), '`', '''), ``,
ENGINE=InnoDB,
ALGORITHM=COPY;') AS Query
FROM INFORMATION_SCHEMA.INNODB_TABLES
WHERE SPACE <> 0 AND LEFT(NAME, INSTR((NAME), '/') - 1) NOT IN ('mysql','');
```

Rebuilding a MySQL table to move the table's metadata to the shared tablespace requires additional storage space temporarily to rebuild the table, so the DB instance must have storage space available.

During rebuilding, the table is locked and inaccessible to queries. For small tables or tables not frequently accessed, this might not be an issue. For large tables or tables frequently accessed in a heavily concurrent environment, you can rebuild tables on a read replica.

You can create a read replica and migrate table metadata to the shared tablespace on the read replica. While the ALTER TABLE statement blocks access on the read replica, the source DB instance is not affected. The source DB instance will continue to generate its binary logs while the read replica lags during the table rebuilding process. Because the rebuilding requires additional storage space and the replay log file can become large, you should create a read replica with storage allocated that is larger than the source DB instance.

To create a read replica and rebuild InnoDB tables to use the shared tablespace, take the following steps:

1. Make sure that backup retention is enabled on the source DB instance so that binary logging is enabled.
2. Use the AWS Management Console or AWS CLI to create a read replica for the source DB instance. Because the creation of a read replica involves many of the same processes as crash recovery, the creation process can take some time if there is a large number of InnoDB tablespaces. Allocate more storage space on the read replica than is currently used on the source DB instance.
3. When the read replica has been created, create a parameter group with the parameter settings `read_only = 0` and `innodb_file_per_table = 0`. Then associate the parameter group with the read replica.
4. Issue the following SQL statement for all tables that you want migrated on the replica:

```
ALTER TABLE name ENGINE = InnoDB
```

5. When all of your ALTER TABLE statements have completed on the read replica, verify that the read replica is connected to the source DB instance and that the two instances are in sync.
6. Use the console or CLI to promote the read replica to be the instance. Make sure that the parameter group used for the new standalone DB instance has the `innodb_file_per_table` parameter set to 0. Change the name of the new standalone DB instance, and point any applications to the new standalone DB instance.

Managing the global status history

MySQL maintains many status variables that provide information about its operation. Their value can help you detect locking or memory issues on a DB instance . The values of these status variables are cumulative since last time the DB instance was started. You can reset most status variables to 0 by using the FLUSH STATUS command.

To allow for monitoring of these values over time, Amazon RDS provides a set of procedures that will snapshot the values of these status variables over time and write them to a table, along with any changes since the last snapshot. This infrastructure, called Global Status History (GoSH), is installed on all MySQL DB instances starting with versions 5.5.23. GoSH is disabled by default.

To enable GoSH, you first enable the event scheduler from a DB parameter group by setting the parameter `event_scheduler` to ON. For information about creating and modifying a DB parameter group, see [Working with parameter groups \(p. 289\)](#).

You can then use the procedures in the following table to enable and configure GoSH. First connect to your MySQL DB instance, then issue the appropriate commands as shown following. For more information, see [Connecting to a DB instance running the MySQL database engine \(p. 1318\)](#). For each procedure, type the following:

```
CALL procedure-name;
```

Where *procedure-name* is one of the procedures in the table.

Procedure	Description
<code>mysql.rds_enable_gsh_collector</code>	Enables GoSH to take default snapshots at intervals specified by <code>rds_set_gsh_collector</code> .
<code>mysql.rds_set_gsh_collector</code>	Specifies the interval, in minutes, between snapshots. Default value is 5.
<code>mysql.rds_disable_gsh_collector</code>	Disables snapshots.
<code>mysql.rds_collect_global_status</code>	Takes a snapshot on demand.
<code>mysql.rds_enable_gsh_rotation</code>	Enables rotation of the contents of the <code>mysql.rds_global_status_history</code> table to <code>mysql.rds_global_status_history_old</code> at intervals specified by <code>rds_set_gsh_rotation</code> .
<code>mysql.rds_set_gsh_rotation</code>	Specifies the interval, in days, between table rotations. Default value is 7.
<code>mysql.rds_disable_gsh_rotation</code>	Disables table rotation.
<code>mysql.rds_rotate_global_status</code>	Rotates the contents of the <code>mysql.rds_global_status_history</code> table to <code>mysql.rds_global_status_history_old</code> on demand.

When GoSH is running, you can query the tables that it writes to. For example, to query the hit ratio of the Innodb buffer pool, you would issue the following query:

```
select a.collection_end, a.collection_start, (( a.variable_Delta-b.variable_delta)/
a.variable_delta)*100 as "HitRatio"
    from mysql.rds_global_status_history as a join mysql.rds_global_status_history as b on
a.collection_end = b.collection_end
      where a. variable_name = 'Innodb_buffer_pool_read_requests' and b.variable_name =
'Innodb_buffer_pool_reads'
```

Local time zone for MySQL DB instances

By default, the time zone for a MySQL DB instance is Universal Time Coordinated (UTC). You can set the time zone for your DB instance to the local time zone for your application instead.

To set the local time zone for a DB instance, set the `time_zone` parameter in the parameter group for your DB instance to one of the supported values listed later in this section. When you set the `time_zone` parameter for a parameter group, all DB instances and read replicas that are using that parameter group change to use the new local time zone. For information on setting parameters in a parameter group, see [Working with parameter groups \(p. 289\)](#).

After you set the local time zone, all new connections to the database reflect the change. If you have any open connections to your database when you change the local time zone, you won't see the local time zone update until after you close the connection and open a new connection.

You can set a different local time zone for a DB instance and one or more of its read replicas. To do this, use a different parameter group for the DB instance and the replica or replicas and set the `time_zone` parameter in each parameter group to a different local time zone.

If you are replicating across AWS Regions, then the source DB instance and the read replica use different parameter groups (parameter groups are unique to an AWS Region). To use the same local time zone for each instance, you must set the `time_zone` parameter in the instance's and read replica's parameter groups.

When you restore a DB instance from a DB snapshot, the local time zone is set to UTC. You can update the time zone to your local time zone after the restore is complete. If you restore a DB instance to a point in time, then the local time zone for the restored DB instance is the time zone setting from the parameter group of the restored DB instance.

You can set your local time zone to one of the following values.

Africa/Cairo	Asia/Riyadh
Africa/Casablanca	Asia/Seoul
Africa/Harare	Asia/Shanghai
Africa/Monrovia	Asia/Singapore
Africa/Nairobi	Asia/Taipei
Africa/Tripoli	Asia/Tehran
Africa/Windhoek	Asia/Tokyo
America/Araguaina	Asia/Ulaanbaatar
America/Asuncion	Asia/Vladivostok
America/Bogota	Asia/Yakutsk
America/Buenos_Aires	Asia/Yerevan
America/Caracas	Atlantic/Azores
America/Chihuahua	Australia/Adelaide
America/Cuiaba	Australia/Brisbane

America/Denver	Australia/Darwin
America/Fortaleza	Australia/Hobart
America/Guatemala	Australia/Perth
America/Halifax	Australia/Sydney
America/Manaus	Brazil/East
America/Matamoros	Canada/Newfoundland
America/Monterrey	Canada/Saskatchewan
America/Montevideo	Canada/Yukon
America/Phoenix	Europe/Amsterdam
America/Santiago	Europe/Athens
America/Tijuana	Europe/Dublin
Asia/Amman	Europe/Helsinki
Asia/Ashgabat	Europe/Istanbul
Asia/Baghdad	Europe/Kaliningrad
Asia/Baku	Europe/Moscow
Asia/Bangkok	Europe/Paris
Asia/Beirut	Europe/Prague
Asia/Calcutta	Europe/Sarajevo
Asia/Damascus	Pacific/Auckland
Asia/Dhaka	Pacific/Fiji
Asia/Irkutsk	Pacific/Guam
Asia/Jerusalem	Pacific/Honolulu
Asia/Kabul	Pacific/Samoa
Asia/Karachi	US/Alaska
Asia/Kathmandu	US/Central
Asia/Krasnoyarsk	US/Eastern
Asia/Magadan	US/East-Indiana
Asia/Muscat	US/Pacific
Asia/Novosibirsk	UTC

Known issues and limitations for Amazon RDS for MySQL

Known issues and limitations for working with Amazon RDS for MySQL are as follows.

Topics

- [InnoDB reserved word \(p. 1435\)](#)
- [Storage-full behavior for Amazon RDS for MySQL \(p. 1435\)](#)
- [Inconsistent InnoDB buffer pool size \(p. 1436\)](#)
- [Index merge optimization returns incorrect results \(p. 1436\)](#)
- [Log file size \(p. 1437\)](#)
- [MySQL parameter exceptions for Amazon RDS DB instances \(p. 1437\)](#)
- [MySQL file size limits in Amazon RDS \(p. 1437\)](#)
- [MySQL Keyring Plugin not supported \(p. 1438\)](#)

InnoDB reserved word

InnoDB is a reserved word for RDS for MySQL. You can't use this name for a MySQL database.

Storage-full behavior for Amazon RDS for MySQL

When storage becomes full for a MySQL DB instance, there can be metadata inconsistencies, dictionary mismatches, and orphan tables. To prevent these issues, Amazon RDS automatically stops a DB instance that reaches the `storage-full` state.

A MySQL DB instance reaches the `storage-full` state in the following cases:

- The DB instance has less than 20,000 MiB of storage, and available storage reaches 200 MiB or less.
- The DB instance has more than 102,400 MiB of storage, and available storage reaches 1024 MiB or less.
- The DB instance has between 20,000 MiB and 102,400 MiB of storage, and has less than 1% of storage available.

After Amazon RDS stops a DB instance automatically because it reached the `storage-full` state, you can still modify it. To restart the DB instance, complete at least one of the following:

- Modify the DB instance to enable storage autoscaling.

For more information about storage autoscaling, see [Managing capacity automatically with Amazon RDS storage autoscaling \(p. 412\)](#).

- Modify the DB instance to increase its storage capacity.

For more information about increasing storage capacity, see [Increasing DB instance storage capacity \(p. 410\)](#).

After you make one of these changes, the DB instance is restarted automatically. For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Inconsistent InnoDB buffer pool size

For MySQL 5.7, there is currently a bug in the way that the InnoDB buffer pool size is managed. MySQL 5.7 might adjust the value of the `innodb_buffer_pool_size` parameter to a large value that can result in the InnoDB buffer pool growing too large and using up too much memory. This effect can cause the MySQL database engine to stop running or can prevent the MySQL database engine from starting. This issue is more common for DB instance classes that have less memory available.

To resolve this issue, set the value of the `innodb_buffer_pool_size` parameter to a multiple of the product of the `innodb_buffer_pool_instances` parameter value and the `innodb_buffer_pool_chunk_size` parameter value. For example, you might set the `innodb_buffer_pool_size` parameter value to a multiple of eight times the product of the `innodb_buffer_pool_instances` and `innodb_buffer_pool_chunk_size` parameter values, as shown in the following example.

```
innodb_buffer_pool_chunk_size = 536870912
innodb_buffer_pool_instances = 4
innodb_buffer_pool_size = (536870912 * 4) * 8 = 17179869184
```

For details on this MySQL 5.7 bug, see <https://bugs.mysql.com/bug.php?id=79379> in the MySQL documentation.

Index merge optimization returns incorrect results

Queries that use index merge optimization might return incorrect results due to a bug in the MySQL query optimizer that was introduced in MySQL 5.5.37. When you issue a query against a table with multiple indexes the optimizer scans ranges of rows based on the multiple indexes, but does not merge the results together correctly. For more information on the query optimizer bug, see <http://bugs.mysql.com/bug.php?id=72745> and <http://bugs.mysql.com/bug.php?id=68194> in the MySQL bug database.

For example, consider a query on a table with two indexes where the search arguments reference the indexed columns.

```
SELECT * FROM table1
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

In this case, the search engine will search both indexes. However, due to the bug, the merged results are incorrect.

To resolve this issue, you can do one of the following:

- Set the `optimizer_switch` parameter to `index_merge=off` in the DB parameter group for your MySQL DB instance. For information on setting DB parameter group parameters, see [Working with parameter groups \(p. 289\)](#).
- Upgrade your MySQL DB instance to MySQL version 5.7 or 8.0. For more information, see [Upgrading a MySQL DB snapshot \(p. 1353\)](#).
- If you cannot upgrade your instance or change the `optimizer_switch` parameter, you can work around the bug by explicitly identifying an index for the query, for example:

```
SELECT * FROM table1
USE INDEX covering_index
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

For more information, see [Index merge optimization](#) in the MySQL documentation.

Log file size

For MySQL, there is a size limit on BLOBS written to the redo log. To account for this limit, ensure that the `innodb_log_file_size` parameter for your MySQL DB instance is 10 times larger than the largest BLOB data size found in your tables, plus the length of other variable length fields (VARCHAR, VARBINARY, TEXT) in the same tables. For information on how to set parameter values, see [Working with parameter groups \(p. 289\)](#). For information on the redo log BLOB size limit, see [Changes in MySQL 5.6.20](#).

MySQL parameter exceptions for Amazon RDS DB instances

Some MySQL parameters require special considerations when used with an Amazon RDS DB instance.

`lower_case_table_names`

Because Amazon RDS uses a case-sensitive file system, setting the value of the `lower_case_table_names` server parameter to 2 ("names stored as given but compared in lowercase") is not supported. The following are the supported values for Amazon RDS for MySQL DB instances:

- 0 ("names stored as given and comparisons are case-sensitive") is supported for all Amazon RDS for MySQL versions.
- 1 ("names stored in lowercase and comparisons are not case-sensitive") is supported for RDS for MySQL version 5.7 and version 8.0.23 and higher 8.0 versions.

Set the `lower_case_table_names` parameter in a custom DB parameter group before creating a DB instance. Then, specify the custom DB parameter group when you create the DB instance.

When a parameter group is associated with a MySQL DB instance with a version lower than 8.0, we recommend that you avoid changing the `lower_case_table_names` parameter in the parameter group. Doing so could cause inconsistencies with point-in-time recovery backups and read replica DB instances.

When a parameter group is associated with a version 8.0 MySQL DB instance, you can't modify the `lower_case_table_names` parameter in the parameter group.

Read replicas should always use the same `lower_case_table_names` parameter value as the source DB instance.

`long_query_time`

You can set the `long_query_time` parameter to a floating point value which allows you to log slow queries to the MySQL slow query log with microsecond resolution. You can set a value such as 0.1 seconds, which would be 100 milliseconds, to help when debugging slow transactions that take less than one second.

MySQL file size limits in Amazon RDS

For MySQL DB instances, the maximum provisioned storage limit constrains the size of a table to a maximum size of 16 TB when using InnoDB file-per-table tablespaces. This limit also constrains the system tablespace to a maximum size of 16 TB. InnoDB file-per-table tablespaces (with tables each in their own tablespace) is set by default for MySQL DB instances.

Note

Some existing DB instances have a lower limit. For example, MySQL DB instances created before April 2014 have a file and table size limit of 2 TB. This 2 TB file size limit also applies to DB instances or read replicas created from DB snapshots taken before April 2014, regardless of when the DB instance was created.

There are advantages and disadvantages to using InnoDB file-per-table tablespaces, depending on your application. To determine the best approach for your application, see [File-per-table tablespaces](#) in the MySQL documentation.

We don't recommend allowing tables to grow to the maximum file size. In general, a better practice is to partition data into smaller tables, which can improve performance and recovery times.

One option that you can use for breaking a large table up into smaller tables is partitioning. Partitioning distributes portions of your large table into separate files based on rules that you specify. For example, if you store transactions by date, you can create partitioning rules that distribute older transactions into separate files using partitioning. Then periodically, you can archive the historical transaction data that doesn't need to be readily available to your application. For more information, see [Partitioning](#) in the MySQL documentation.

To determine the file size of a table

- Use the following SQL command to determine if any of your tables are too large and are candidates for partitioning.

```
SELECT TABLE_SCHEMA, TABLE_NAME,
round(((DATA_LENGTH + INDEX_LENGTH) / 1024 / 1024), 2) As "Approximate size (MB)"
FROM information_schema.TABLES
WHERE TABLE_SCHEMA NOT IN ('mysql', 'information_schema', 'performance_schema');
```

To enable InnoDB file-per-table tablespaces

- To enable InnoDB file-per-table tablespaces, set the *innodb_file_per_table* parameter to 1 in the parameter group for the DB instance.

To disable InnoDB file-per-table tablespaces

- To disable InnoDB file-per-table tablespaces, set the *innodb_file_per_table* parameter to 0 in the parameter group for the DB instance.

For information on updating a parameter group, see [Working with parameter groups \(p. 289\)](#).

When you have enabled or disabled InnoDB file-per-table tablespaces, you can issue an ALTER TABLE command to move a table from the global tablespace to its own tablespace, or from its own tablespace to the global tablespace as shown in the following example:

```
ALTER TABLE table_name ENGINE=InnoDB;
```

MySQL Keyring Plugin not supported

Currently, Amazon RDS for MySQL does not support the MySQL keyring_aws Amazon Web Services Keyring Plugin.

MySQL on Amazon RDS SQL reference

Following, you can find a description of system stored procedures that are available for Amazon RDS instances running the MySQL DB engine.

Overview

The following system stored procedures are supported for Amazon RDS DB instances running MySQL. The master user must run these procedures.

Replication

- [mysql.rds_set_master_auto_position \(p. 1440\)](#)
- [mysql.rds_set_external_master \(p. 1441\)](#)
- [mysql.rds_set_external_master_with_delay \(p. 1443\)](#)
- [mysql.rds_set_external_master_with_auto_position \(p. 1446\)](#)
- [mysql.rds_reset_external_master \(p. 1448\)](#)
- [mysql.rds_import_binlog_ssl_material \(p. 1449\)](#)
- [mysql.rds_remove_binlog_ssl_material \(p. 1451\)](#)
- [mysql.rds_set_source_delay \(p. 1451\)](#)
- [mysql.rds_start_replication \(p. 1452\)](#)
- [mysql.rds_start_replication_until \(p. 1452\)](#)
- [mysql.rds_start_replication_until_gtid \(p. 1453\)](#)
- [mysql.rds_stop_replication \(p. 1454\)](#)
- [mysql.rds_skip_transaction_with_gtid \(p. 1455\)](#)
- [mysql.rds_skip_repl_error \(p. 1455\)](#)
- [mysql.rds_next_master_log \(p. 1456\)](#)

InnoDB cache warming

- [mysql.rds_innodb_buffer_pool_dump_now \(p. 1458\)](#)
- [mysql.rds_innodb_buffer_pool_load_now \(p. 1458\)](#)
- [mysql.rds_innodb_buffer_pool_load_abort \(p. 1459\)](#)

Managing additional configuration (for example, binlog file retention)

- [mysql.rds_set_configuration \(p. 1459\)](#)
- [mysql.rds_show_configuration \(p. 1460\)](#)

Ending a session or query

- [mysql.rds_kill \(p. 1461\)](#)
- [mysql.rds_kill_query \(p. 1461\)](#)

Logging

- [mysql.rds_rotate_general_log \(p. 1462\)](#)
- [mysql.rds_rotate_slow_log \(p. 1462\)](#)

Managing the global status history

- [mysql.rds_enable_gsh_collector \(p. 1463\)](#)
- [mysql.rds_set_gsh_collector \(p. 1463\)](#)
- [mysql.rds_disable_gsh_collector \(p. 1463\)](#)
- [mysql.rds_collect_global_status_history \(p. 1463\)](#)
- [mysql.rds_enable_gsh_rotation \(p. 1464\)](#)
- [mysql.rds_set_gsh_rotation \(p. 1464\)](#)
- [mysql.rds_disable_gsh_rotation \(p. 1464\)](#)
- [mysql.rds_rotate_global_status_history \(p. 1464\)](#)

SQL reference conventions

Following, you can find explanations for the conventions that are used to describe the syntax of the system stored procedures and tables described in the SQL reference section.

Character	Description
UPPERCASE	Words in uppercase are keywords.
[]	Square brackets indicate optional arguments.
{ }	Braces indicate that you are required to choose one of the arguments inside the braces.
	Pipes separate arguments that you can choose.
<i>italics</i>	Words in italics indicate placeholders. You must insert the appropriate value in place of the word in italics.
...	An ellipsis indicates that you can repeat the preceding element.
'	Words in single quotes indicate that you must type the quotes.

mysql.rds_set_master_auto_position

Sets the replication mode to be based on either binary log file positions or on global transaction identifiers (GTIDs).

Syntax

```
CALL mysql.rds_set_master_auto_position (
    auto_position_mode
);
```

Parameters

auto_position_mode

A value that indicates whether to use log file position replication or GTID-based replication:

- 0 – Use the replication method based on binary log file position. The default is 0.

- 1 – Use the GTID-based replication method.

Usage notes

The master user must run the `mysql.rds_set_master_auto_position` procedure.

This procedure is supported for all RDS for MySQL 5.7 versions, and RDS for MySQL 8.0.26 and higher 8.0 versions.

mysql.rds_set_external_master

Configures a MySQL DB instance to be a read replica of an instance of MySQL running external to Amazon RDS.

Important

To run this procedure, `autocommit` must be enabled. To enable it, set the `autocommit` parameter to 1. For information about modifying parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Note

You can use the [mysql.rds_set_external_master_with_delay \(p. 1443\)](#) stored procedure to configure an external source database instance and delayed replication.

Syntax

```
CALL mysql.rds_set_external_master (
    host_name
    , host_port
    , replication_user_name
    , replication_user_password
    , mysql_binary_log_file_name
    , mysql_binary_log_file_location
    , ssl_encryption
);
```

Parameters

host_name

The host name or IP address of the MySQL instance running external to Amazon RDS to become the source database instance.

host_port

The port used by the MySQL instance running external to Amazon RDS to be configured as the source database instance. If your network configuration includes Secure Shell (SSH) port replication that converts the port number, specify the port number that is exposed by SSH.

replication_user_name

The ID of a user with `REPLICATION CLIENT` and `REPLICATION SLAVE` permissions on the MySQL instance running external to Amazon RDS. We recommend that you provide an account that is used solely for replication with the external instance.

replication_user_password

The password of the user ID specified in `replication_user_name`.

mysql_binary_log_file_name

The name of the binary log on the source database instance that contains the replication information.

mysql_binary_log_file_location

The location in the *mysql_binary_log_file_name* binary log at which replication starts reading the replication information.

You can determine the binlog file name and location by running `SHOW MASTER STATUS` on the source database instance.

ssl_encryption

A value that specifies whether Secure Socket Layer (SSL) encryption is used on the replication connection. 1 specifies to use SSL encryption, 0 specifies to not use encryption. The default is 0.

Note

The `MASTER_SSL_VERIFY_SERVER_CERT` option isn't supported. This option is set to 0, which means that the connection is encrypted, but the certificates aren't verified.

Usage notes

The master user must run the `mysql.rds_set_external_master` procedure. This procedure must be run on the MySQL DB instance to be configured as the read replica of a MySQL instance running external to Amazon RDS.

Before you run `mysql.rds_set_external_master`, you must configure the instance of MySQL running external to Amazon RDS to be a source database instance. To connect to the MySQL instance running external to Amazon RDS, you must specify `replication_user_name` and `replication_user_password` values that indicate a replication user that has `REPLICATION CLIENT` and `REPLICATION SLAVE` permissions on the external instance of MySQL.

To configure an external instance of MySQL as a source database instance

1. Using the MySQL client of your choice, connect to the external instance of MySQL and create a user account to be used for replication. The following is an example.

MySQL 5.7

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

MySQL 8.0

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY 'password';
```

2. On the external instance of MySQL, grant `REPLICATION CLIENT` and `REPLICATION SLAVE` privileges to your replication user. The following example grants `REPLICATION CLIENT` and `REPLICATION SLAVE` privileges on all databases for the 'repl_user' user for your domain.

MySQL 5.7

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'  
IDENTIFIED BY 'password';
```

MySQL 8.0

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

To use encrypted replication, configure source database instance to use SSL connections. Also, import the certificate authority certificate, client certificate, and client key into the DB instance or DB cluster using the [mysql.rds_import_binlog_ssl_material \(p. 1449\)](#) procedure.

Note

We recommend that you use read replicas to manage replication between two Amazon RDS DB instances when possible. When you do so, we recommend that you use only this and other replication-related stored procedures. These practices enable more complex replication topologies between Amazon RDS DB instances. We offer these stored procedures primarily to enable replication with MySQL instances running external to Amazon RDS. For information about managing replication between Amazon RDS DB instances, see [Working with read replicas \(p. 370\)](#).

After calling `mysql.rds_set_external_master` to configure an Amazon RDS DB instance as a read replica, you can call [mysql.rds_start_replication \(p. 1452\)](#) on the read replica to start the replication process. You can call [mysql.rds_reset_external_master \(p. 1448\)](#) to remove the read replica configuration.

When `mysql.rds_set_external_master` is called, Amazon RDS records the time, user, and an action of `set master` in the `mysql.rds_history` and `mysql.rds_replication_status` tables.

Examples

When run on a MySQL DB instance, the following example configures the DB instance to be a read replica of an instance of MySQL running external to Amazon RDS.

```
call mysql.rds_set_external_master(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.0777',
  120,
  0);
```

mysql.rds_set_external_master_with_delay

Configures an RDS for MySQL DB instance to be a read replica of an instance of MySQL running external to Amazon RDS and configures delayed replication.

Important

To run this procedure, `autocommit` must be enabled. To enable it, set the `autocommit` parameter to 1. For information about modifying parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Syntax

```
CALL mysql.rds_set_external_master_with_delay (
  host_name
  , host_port
  , replication_user_name
```

```
, replication_user_password
, mysql_binary_log_file_name
, mysql_binary_log_file_location
, ssl_encryption
, delay
);
```

Parameters

host_name

The host name or IP address of the MySQL instance running external to Amazon RDS that will become the source database instance.

host_port

The port used by the MySQL instance running external to Amazon RDS to be configured as the source database instance. If your network configuration includes SSH port replication that converts the port number, specify the port number that is exposed by SSH.

replication_user_name

The ID of a user with REPLICATION CLIENT and REPLICATION SLAVE permissions on the MySQL instance running external to Amazon RDS. We recommend that you provide an account that is used solely for replication with the external instance.

replication_user_password

The password of the user ID specified in *replication_user_name*.

mysql_binary_log_file_name

The name of the binary log on the source database instance contains the replication information.

mysql_binary_log_file_location

The location in the *mysql_binary_log_file_name* binary log at which replication will start reading the replication information.

You can determine the binlog file name and location by running SHOW MASTER STATUS on the source database instance.

ssl_encryption

A value that specifies whether Secure Socket Layer (SSL) encryption is used on the replication connection. 1 specifies to use SSL encryption, 0 specifies to not use encryption. The default is 0.

Note

The MASTER_SSL_VERIFY_SERVER_CERT option isn't supported. This option is set to 0, which means that the connection is encrypted, but the certificates aren't verified.

delay

The minimum number of seconds to delay replication from source database instance.

The limit for this parameter is one day (86400 seconds).

Usage notes

The master user must run the `mysql.rds_set_external_master_with_delay` procedure. This procedure must be run on the MySQL DB instance to be configured as the read replica of a MySQL instance running external to Amazon RDS.

Before you run `mysql.rds_set_external_master_with_delay`, you must configure the instance of MySQL running external to Amazon RDS to be a source database instance. To connect to the MySQL instance running external to Amazon RDS, you must specify values for `replication_user_name` and `replication_user_password`. These values must indicate a replication user that has `REPLICATION CLIENT` and `REPLICATION SLAVE` permissions on the external instance of MySQL.

To configure an external instance of MySQL as a source database instance

1. Using the MySQL client of your choice, connect to the external instance of MySQL and create a user account to be used for replication. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
```

2. On the external instance of MySQL, grant `REPLICATION CLIENT` and `REPLICATION SLAVE` privileges to your replication user. The following example grants `REPLICATION CLIENT` and `REPLICATION SLAVE` privileges on all databases for the '`repl_user`' user for your domain.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'  
IDENTIFIED BY 'SomePassW0rd'
```

For more information, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#).

Note

We recommend that you use read replicas to manage replication between two Amazon RDS DB instances when possible. When you do so, we recommend that you use only this and other replication-related stored procedures. These practices enable more complex replication topologies between Amazon RDS DB instances. We offer these stored procedures primarily to enable replication with MySQL instances running external to Amazon RDS. For information about managing replication between Amazon RDS DB instances, see [Working with read replicas \(p. 370\)](#).

After calling `mysql.rds_set_external_master_with_delay` to configure an Amazon RDS DB instance as a read replica, you can call [mysql.rds_start_replication \(p. 1452\)](#) on the read replica to start the replication process. You can call [mysql.rds_reset_external_master \(p. 1448\)](#) to remove the read replica configuration.

When you call `mysql.rds_set_external_master_with_delay`, Amazon RDS records the time, the user, and an action of `set master` in the `mysql.rds_history` and `mysql.rds_replication_status` tables.

For disaster recovery, you can use this procedure with the [mysql.rds_start_replication_until \(p. 1452\)](#) or [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure. To roll forward changes to a delayed read replica to the time just before a disaster, you can run the `mysql.rds_set_external_master_with_delay` procedure. After the `mysql.rds_start_replication_until` procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

To use the `mysql.rds_start_replication_until_gtid` procedure, GTID-based replication must be enabled. To skip a specific GTID-based transaction that is known to cause disaster, you can use the [mysql.rds_skip_transaction_with_gtid \(p. 1455\)](#) stored procedure. For more information about working with GTID-based replication, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

The `mysql.rds_set_external_master_with_delay` procedure is available in these versions of RDS for MySQL:

- MySQL 8.0.26 and higher 8.0 versions
- All 5.7 versions

Examples

When run on a MySQL DB instance, the following example configures the DB instance to be a read replica of an instance of MySQL running external to Amazon RDS. It sets the minimum replication delay to one hour (3,600 seconds) on the MySQL DB instance. A change from the MySQL source database instance running external to Amazon RDS isn't applied on the MySQL DB instance read replica for at least one hour.

```
call mysql.rds_set_external_master_with_delay(
    'Externaldb.some.com',
    3306,
    'repl_user',
    'SomePassW0rd',
    'mysql-bin-changelog.000777',
    120,
    0,
    3600);
```

mysql.rds_set_external_master_with_auto_position

Configures an RDS for MySQL DB instance to be a read replica of an instance of MySQL running external to Amazon RDS. This procedure also configures delayed replication and replication based on global transaction identifiers (GTIDs).

Important

To run this procedure, autocommit must be enabled. To enable it, set the autocommit parameter to 1. For information about modifying parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Syntax

```
CALL mysql.rds_set_external_master_with_auto_position (
    host_name
    , host_port
    , replication_user_name
    , replication_user_password
    , ssl_encryption
    , delay
);
```

Parameters

host_name

The host name or IP address of the MySQL instance running external to Amazon RDS to become the source database instance.

host_port

The port used by the MySQL instance running external to Amazon RDS to be configured as the source database instance. If your network configuration includes Secure Shell (SSH) port replication that converts the port number, specify the port number that is exposed by SSH.

replication_user_name

The ID of a user with REPLICATION CLIENT and REPLICATION SLAVE permissions on the MySQL instance running external to Amazon RDS. We recommend that you provide an account that is used solely for replication with the external instance.

replication_user_password

The password of the user ID specified in `replication_user_name`.

ssl_encryption

A value that specifies whether Secure Socket Layer (SSL) encryption is used on the replication connection. 1 specifies to use SSL encryption, 0 specifies to not use encryption. The default is 0.

Note

The `MASTER_SSL_VERIFY_SERVER_CERT` option isn't supported. This option is set to 0, which means that the connection is encrypted, but the certificates aren't verified.

delay

The minimum number of seconds to delay replication from source database instance.

The limit for this parameter is one day (86,400 seconds).

Usage notes

The master user must run the `mysql.rds_set_external_master_with_auto_position` procedure. This procedure must be run on the MySQL DB instance to be configured as the read replica of a MySQL instance running external to Amazon RDS.

This procedure is supported for all RDS for MySQL 5.7 versions, and RDS for MySQL 8.0.26 and higher 8.0 versions.

Before you run `mysql.rds_set_external_master_with_auto_position`, you must configure the instance of MySQL running external to Amazon RDS to be a source database instance. To connect to the MySQL instance running external to Amazon RDS, you must specify values for `replication_user_name` and `replication_user_password`. These values must indicate a replication user that has REPLICATION CLIENT and REPLICATION SLAVE permissions on the external instance of MySQL.

To configure an external instance of MySQL as a source database instance

1. Using the MySQL client of your choice, connect to the external instance of MySQL and create a user account to be used for replication. The following is an example.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
```

2. On the external instance of MySQL, grant REPLICATION CLIENT and REPLICATION SLAVE privileges to your replication user. The following example grants REPLICATION CLIENT and REPLICATION SLAVE privileges on all databases for the '`repl_user`' user for your domain.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'  
IDENTIFIED BY 'SomePassW0rd'
```

For more information, see [Configuring binary log file position replication with an external source instance \(p. 1408\)](#).

Note

We recommend that you use read replicas to manage replication between two Amazon RDS DB instances when possible. When you do so, we recommend that you use only this and

other replication-related stored procedures. These practices enable more complex replication topologies between Amazon RDS DB instances. We offer these stored procedures primarily to enable replication with MySQL instances running external to Amazon RDS. For information about managing replication between Amazon RDS DB instances, see [Working with read replicas \(p. 370\)](#).

After calling `mysql.rds_set_external_master_with_auto_position` to configure an Amazon RDS DB instance as a read replica, you can call [mysql.rds_start_replication \(p. 1452\)](#) on the read replica to start the replication process. You can call [mysql.rds_reset_external_master \(p. 1448\)](#) to remove the read replica configuration.

When you call `mysql.rds_set_external_master_with_auto_position`, Amazon RDS records the time, the user, and an action of `set master` in the `mysql.rds_history` and `mysql.rds_replication_status` tables.

For disaster recovery, you can use this procedure with the [mysql.rds_start_replication_until \(p. 1452\)](#) or [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure. To roll forward changes to a delayed read replica to the time just before a disaster, you can run the `mysql.rds_set_external_master_with_auto_position` procedure. After the `mysql.rds_start_replication_until_gtid` procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

To use the `mysql.rds_start_replication_until_gtid` procedure, GTID-based replication must be enabled. To skip a specific GTID-based transaction that is known to cause disaster, you can use the [mysql.rds_skip_transaction_with_gtid \(p. 1455\)](#) stored procedure. For more information about working with GTID-based replication, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

Examples

When run on a MySQL DB instance, the following example configures the DB instance to be a read replica of an instance of MySQL running external to Amazon RDS. It sets the minimum replication delay to one hour (3,600 seconds) on the MySQL DB instance. A change from the MySQL source database instance running external to Amazon RDS isn't applied on the MySQL DB instance read replica for at least one hour.

```
call mysql.rds_set_external_master_with_auto_position(
    'Externaldb.some.com',
    3306,
    'repl_user',
    'SomePassW0rd',
    0,
    3600);
```

mysql.rds_reset_external_master

Reconfigures a MySQL DB instance to no longer be a read replica of an instance of MySQL running external to Amazon RDS.

Important

To run this procedure, `autocommit` must be enabled. To enable it, set the `autocommit` parameter to 1. For information about modifying parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Syntax

```
CALL mysql.rds_reset_external_master;
```

Usage notes

The master user must run the `mysql.rds_reset_external_master` procedure. This procedure must be run on the MySQL DB instance to be removed as a read replica of a MySQL instance running external to Amazon RDS.

Note

We recommend that you use read replicas to manage replication between two Amazon RDS DB instances when possible. When you do so, we recommend that you use only this and other replication-related stored procedures. These practices enable more complex replication topologies between Amazon RDS DB instances. We offer these stored procedures primarily to enable replication with MySQL instances running external to Amazon RDS. For information about managing replication between Amazon RDS DB instances, see [Working with read replicas \(p. 370\)](#).

For more information about using replication to import data from an instance of MySQL running external to Amazon RDS, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

mysql.rds_import_binlog_ssl_material

Imports the certificate authority certificate, client certificate, and client key into an Aurora MySQL DB cluster. The information is required for SSL communication and encrypted replication.

Note

Currently, this procedure is supported for Aurora MySQL version 1; version 2: 2.09.2, 2.10.0, 2.10.1, and 2.11.0; and version 3: 3.01.1 and higher.

Syntax

```
CALL mysql.rds_import_binlog_ssl_material (
    ssl_material
);
```

Parameters

ssl_material

JSON payload that contains the contents of the following .pem format files for a MySQL client:

- "ssl_ca": "*Certificate authority certificate*"
- "ssl_cert": "*Client certificate*"
- "ssl_key": "*Client key*"

Usage notes

Prepare for encrypted replication before you run this procedure:

- If you don't have SSL enabled on the external MySQL source database instance and don't have a client key and client certificate prepared, enable SSL on the MySQL database server and generate the required client key and client certificate.
- If SSL is enabled on the external source database instance, supply a client key and certificate for the Aurora MySQL DB cluster. If you don't have these, generate a new key and certificate for the Aurora

MySQL DB cluster. To sign the client certificate, you must have the certificate authority key you used to configure SSL on the external MySQL source database instance.

For more information, see [Creating SSL certificates and keys using openssl](#) in the MySQL documentation.

Important

After you prepare for encrypted replication, use an SSL connection to run this procedure. The client key must not be transferred across an insecure connection.

This procedure imports SSL information from an external MySQL database into an Aurora MySQL DB cluster. The SSL information is in .pem format files that contain the SSL information for the Aurora MySQL DB cluster. During encrypted replication, the Aurora MySQL DB cluster acts a client to the MySQL database server. The certificates and keys for the Aurora MySQL client are in files in .pem format.

You can copy the information from these files into the `ssl_material` parameter in the correct JSON payload. To support encrypted replication, import this SSL information into the Aurora MySQL DB cluster.

The JSON payload must be in the following format.

```
'{"ssl_ca":"-----BEGIN CERTIFICATE-----  
ssl_ca_pem_body_code  
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----  
ssl_cert_pem_body_code  
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----  
ssl_key_pem_body_code  
-----END RSA PRIVATE KEY-----\n"}'
```

Examples

The following example imports SSL information into an Aurora MySQL DB cluster. In .pem format files, the body code typically is longer than the body code shown in the example.

```
call mysql.rds_import_binlog_ssl_material(  
'{"ssl_ca":"-----BEGIN CERTIFICATE-----  
AAAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4xyb/wB96xbiFveSFJu0p/d6RjhJ0I0iBXr  
1sLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE  
-----END CERTIFICATE-----\n","ssl_cert":"-----BEGIN CERTIFICATE-----  
AAAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4xyb/wB96xbiFveSFJu0p/d6RjhJ0I0iBXr  
1sLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE  
-----END CERTIFICATE-----\n","ssl_key":"-----BEGIN RSA PRIVATE KEY-----  
AAAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzo0WbkM4xyb/wB96xbiFveSFJu0p/d6RjhJ0I0iBXr  
1sLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb70z1PnW0yN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE  
-----END RSA PRIVATE KEY-----\n"}');
```

Note

For information about using Amazon Aurora, see the [Amazon Aurora User Guide](#).

mysql.rds_remove_binlog_ssl_material

Removes the certificate authority certificate, client certificate, and client key for SSL communication and encrypted replication. This information is imported by using [mysql.rds_import_binlog_ssl_material \(p. 1449\)](#).

Note

Currently, this procedure is only supported for Aurora MySQL version 5.6.

Syntax

```
CALL mysql.rds_remove_binlog_ssl_material;
```

mysql.rds_set_source_delay

Sets the minimum number of seconds to delay replication from source database instance to the current read replica. Use this procedure when you are connected to a read replica to delay replication from its source database instance.

Syntax

```
CALL mysql.rds_set_source_delay(  
    delay  
)
```

Parameters

delay

The minimum number of seconds to delay replication from the source database instance.

The limit for this parameter is one day (86400 seconds).

Usage notes

The master user must run the `mysql.rds_set_source_delay` procedure.

For disaster recovery, you can use this procedure with the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure or the [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure. To roll forward changes to a delayed read replica to the time just before a disaster, you can run the `mysql.rds_set_source_delay` procedure. After the `mysql.rds_start_replication_until` or `mysql.rds_start_replication_until_gtid` procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

To use the `mysql.rds_start_replication_until_gtid` procedure, GTID-based replication must be enabled. To skip a specific GTID-based transaction that is known to cause disaster, you can use the [mysql.rds_skip_transaction_with_gtid \(p. 1455\)](#) stored procedure. For more information on GTID-based replication, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

The `mysql.rds_set_source_delay` procedure is available in these versions of RDS for MySQL:

- MySQL 8.0.26 and higher 8.0 versions

- All 5.7 versions

Examples

To delay replication from source database instance to the current read replica for at least one hour (3,600 seconds), you can call `mysql.rds_set_source_delay` with the following parameter:

```
CALL mysql.rds_set_source_delay(3600);
```

mysql.rds_start_replication

Initiates replication from a MySQL DB instance.

Note

You can use the [mysql.rds_start_replication_until \(p. 1452\)](#) or [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure to initiate replication from an RDS for MySQL DB instance and stop replication at the specified binary log file location.

Syntax

```
CALL mysql.rds_start_replication;
```

Usage notes

The master user must run the `mysql.rds_start_replication` procedure.

If you are configuring replication to import data from an instance of MySQL running external to Amazon RDS, you call `mysql.rds_start_replication` on the read replica to start the replication process after you have called [mysql.rds_set_external_master \(p. 1441\)](#) to build the replication configuration. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

If you are configuring replication to export data to an instance of MySQL external to Amazon RDS, you call `mysql.rds_start_replication` and `mysql.rds_stop_replication` on the read replica to control some replication actions, such as purging binary logs. For more information, see [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

You can also call `mysql.rds_start_replication` on the read replica to restart any replication process that you previously stopped by calling [mysql.rds_stop_replication \(p. 1454\)](#). For more information, see [Working with read replicas \(p. 370\)](#).

mysql.rds_start_replication_until

Initiates replication from an RDS for MySQL DB instance and stops replication at the specified binary log file location.

Syntax

```
CALL mysql.rds_start_replication_until (
  replication_log_file
  , replication_stop_point
);
```

Parameters

replication_log_file

The name of the binary log on the source database instance contains the replication information.

replication_stop_point

The location in the `replication_log_file` binary log at which replication will stop.

Usage notes

The master user must run the `mysql.rds_start_replication_until` procedure.

You can use this procedure with delayed replication for disaster recovery. If you have delayed replication configured, you can use this procedure to roll forward changes to a delayed read replica to the time just before a disaster. After this procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

You can configure delayed replication using the following stored procedures:

- [mysql.rds_set_configuration \(p. 1459\)](#)
- [mysql.rds_set_external_master_with_delay \(p. 1443\)](#)
- [mysql.rds_set_source_delay \(p. 1451\)](#)

The file name specified for the `replication_log_file` parameter must match the source database instance binlog file name.

When the `replication_stop_point` parameter specifies a stop location that is in the past, replication is stopped immediately.

The `mysql.rds_start_replication_until` procedure is available in these versions of RDS for MySQL:

- MySQL 8.0.26 and higher 8.0 versions
- All 5.7 versions

Examples

The following example initiates replication and replicates changes until it reaches location 120 in the `mysql-bin-changelog.000777` binary log file.

```
call mysql.rds_start_replication_until(
    'mysql-bin-changelog.000777',
    120);
```

mysql.rds_start_replication_until_gtid

Initiates replication from an RDS for MySQL DB instance and stops replication immediately after the specified global transaction identifier (GTID).

Syntax

```
CALL mysql.rds_start_replication_until_gtid (
  gtid
);
```

Parameters

gtid

The GTID after which replication is to stop.

Usage notes

The master user must run the `mysql.rds_start_replication_until_gtid` procedure.

This procedure is supported for all RDS for MySQL 5.7 versions, and RDS for MySQL 8.0.26 and higher 8.0 versions.

You can use this procedure with delayed replication for disaster recovery. If you have delayed replication configured, you can use this procedure to roll forward changes to a delayed read replica to the time just before a disaster. After this procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

You can configure delayed replication using the following stored procedures:

- [mysql.rds_set_configuration \(p. 1459\)](#)
- [mysql.rds_set_external_master_with_auto_position \(p. 1446\)](#)
- [mysql.rds_set_source_delay \(p. 1451\)](#)

When the *gtid* parameter specifies a transaction that has already been run by the replica, replication is stopped immediately.

Examples

The following example initiates replication and replicates changes until it reaches GTID 3E11FA47-71CA-11E1-9E33-C80AA9429562:23.

```
call mysql.rds_start_replication_until_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_stop_replication

Stops replication from a MySQL DB instance.

Syntax

```
CALL mysql.rds_stop_replication;
```

Usage notes

The master user must run the `mysql.rds_stop_replication` procedure.

If you are configuring replication to import data from an instance of MySQL running external to Amazon RDS, you call `mysql.rds_stop_replication` on the read replica to stop the replication process

after the import has completed. For more information, see [Restoring a backup into a MySQL DB instance \(p. 1361\)](#).

If you are configuring replication to export data to an instance of MySQL external to Amazon RDS, you call `mysql.rds_start_replication` and `mysql.rds_stop_replication` on the read replica to control some replication actions, such as purging binary logs. For more information, see [Exporting data from a MySQL DB instance by using replication \(p. 1412\)](#).

You can also use `mysql.rds_stop_replication` to stop replication between two Amazon RDS DB instances. You typically stop replication to perform a long running operation on the read replica, such as creating a large index on the read replica. You can restart any replication process that you stopped by calling [mysql.rds_start_replication \(p. 1452\)](#) on the read replica. For more information, see [Working with read replicas \(p. 370\)](#).

mysql.rds_skip_transaction_with_gtid

Skips replication of a transaction with the specified global transaction identifier (GTID) on a MySQL DB instance.

You can use this procedure for disaster recovery when a specific GTID transaction is known to cause a problem. Use this stored procedure to skip the problematic transaction. Examples of problematic transactions include transactions that disable replication, delete important data, or cause the DB instance to become unavailable.

Syntax

```
CALL mysql.rds_skip_transaction_with_gtid (
    gtid_to_skip
);
```

Parameters

gtid_to_skip

The GTID of the replication transaction to skip.

Usage notes

The master user must run the `mysql.rds_skip_transaction_with_gtid` procedure.

This procedure is supported for all RDS for MySQL 5.7 versions, and RDS for MySQL 8.0.26 and higher 8.0 versions.

Examples

The following example skips replication of the transaction with the GTID 3E11FA47-71CA-11E1-9E33-C80AA9429562:23.

```
call mysql.rds_skip_transaction_with_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_skip_repl_error

Skips and deletes a replication error on a MySQL DB instance.

Syntax

```
CALL mysql.rds_skip_repl_error;
```

Usage notes

The master user must run the `mysql.rds_skip_repl_error` procedure.

To determine if there are errors, run the MySQL `SHOW REPLICA STATUS\G` command. If a replication error isn't critical, you can run `mysql.rds_skip_repl_error` to skip the error. If there are multiple errors, `mysql.rds_skip_repl_error` deletes the first error, then warns that others are present. You can then use `SHOW REPLICA STATUS\G` to determine the correct course of action for the next error. For information about the values returned, see [the MySQL documentation](#).

Note

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICA STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

For more information about addressing replication errors with Amazon RDS, see [Troubleshooting a MySQL read replica problem \(p. 1399\)](#).

Replication stopped error

When you call the `mysql.rds_skip_repl_error` command, you might receive an error message stating that the replica is down or disabled.

This error message appears because replication has stopped and could not be restarted.

If you need to skip a large number of errors, the replication lag can increase beyond the default retention period for binary log (binlog) files. In this case, you might encounter a fatal error due to binlog files being purged before they have been replayed on the read replica. This purge causes replication to stop, and you can no longer call the `mysql.rds_skip_repl_error` command to skip replication errors.

You can mitigate this issue by increasing the number of hours that binlog files are retained on your source database instance. After you have increased the binlog retention time, you can restart replication and call the `mysql.rds_skip_repl_error` command as needed.

To set the binlog retention time, use the [mysql.rds_set_configuration \(p. 1459\)](#) procedure and specify a configuration parameter of '`binlog retention hours`' along with the number of hours to retain binlog files on the DB cluster. The following example sets the retention period for binlog files to 48 hours.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

mysql.rds_next_master_log

Changes the source database instance log position to the start of the next binary log on the source database instance. Use this procedure only if you are receiving replication I/O error 1236 on a read replica.

Syntax

```
CALL mysql.rds_next_master_log(
```

```
curr_master_log
);
```

Parameters

curr_master_log

The index of the current master log file. For example, if the current file is named mysql-bin-changelog.012345, then the index is 12345. To determine the current master log file name, run the SHOW REPLICA STATUS command and view the Master_Log_File field.

Note

Previous versions of MySQL used SHOW SLAVE STATUS instead of SHOW REPLICA STATUS. If you are using a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

Usage notes

The master user must run the mysql.rds_next_master_log procedure.

Warning

Call mysql.rds_next_master_log only if replication fails after a failover of a Multi-AZ DB instance that is the replication source, and the Last_IO_Error field of SHOW REPLICA STATUS reports I/O error 1236.

Calling mysql.rds_next_master_log may result in data loss in the read replica if transactions in the source instance were not written to the binary log on disk before the failover event occurred. You can reduce the chance of this happening by configuring the source instance parameters sync_binlog = 1 and innodb_support_xa = 1, although this may reduce performance. For more information, see [Working with read replicas \(p. 370\)](#).

Examples

Assume replication fails on an Amazon RDS read replica. Running SHOW REPLICA STATUS\G on the read replica returns the following result:

```
***** 1. row *****
Replica_IO_State:
  Source_Host: myhostXXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
  Source_User: MasterUser
  Source_Port: 3306
  Connect_Retry: 10
  Source_Log_File: mysql-bin-changelog.012345
  Read_Source_Log_Pos: 1219393
  Relay_Log_File: relaylog.012340
  Relay_Log_Pos: 30223388
  Relay_Source_Log_File: mysql-bin-changelog.012345
  Replica_IO_Running: No
  Replica_SQL_Running: Yes
  Replicate_Do_DB:
  Replicate_Ignore_DB:
  Replicate_Do_Table:
  Replicate_Ignore_Table:
  Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
    Last_Error:
    Skip_Counter: 0
    Last_Error:
    Exec_Source_Log_Pos: 30223232
    Relay_Log_Space: 5248928866
    Until_Condition: None
```

```
    Until_Log_File:
    Until_Log_Pos: 0
    Source_SSL_Allowed: No
    Source_SSL_CA_File:
    Source_SSL_CA_Path:
        Source_SSL_Cert:
        Source_SSL_Cipher:
        Source_SSL_Key:
    Seconds_Behind_Master: NULL
    Source_SSL_Verify_Server_Cert: No
        Last_IO_Errorno: 1236
        Last_IO_Error: Got fatal error 1236 from master when reading data from
binary log: 'Client requested master to start replication from impossible position; the
first event 'mysql-bin-changelog.013406' at 1219393, the last event read from '/rdsdbdata/
log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/rdsdbdata/log/
binlog/mysql-bin-changelog.012345' at 4.'
        Last_SQL_Errorno: 0
        Last_SQL_Error:
    Replicate_Ignore_Server_Ids:
        Source_Server_Id: 67285976
```

The `Last_IO_Errorno` field shows that the instance is receiving I/O error 1236. The `Master_Log_File` field shows that the file name is `mysql-bin-changelog.012345`, which means that the log file index is 12345. To resolve the error, you can call `mysql.rds_next_master_log` with the following parameter:

```
CALL mysql.rds_next_master_log(12345);
```

Note

Previous versions of MySQL used `SHOW SLAVE STATUS` instead of `SHOW REPLICA STATUS`. If you are using a MySQL version before 8.0.23, then use `SHOW SLAVE STATUS`.

mysql.rds_innodb_buffer_pool_dump_now

Dumps the current state of the buffer pool to disk. For more information, see [InnoDB cache warming for MySQL on Amazon RDS \(p. 1313\)](#).

Syntax

```
CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Usage notes

The master user must run the `mysql.rds_innodb_buffer_pool_dump_now` procedure.

mysql.rds_innodb_buffer_pool_load_now

Loads the saved state of the buffer pool from disk. For more information, see [InnoDB cache warming for MySQL on Amazon RDS \(p. 1313\)](#).

Syntax

```
CALL mysql.rds_innodb_buffer_pool_load_now();
```

Usage notes

The master user must run the `mysql.rds_innodb_buffer_pool_load_now` procedure.

mysql.rds_innodb_buffer_pool_load_abort

Cancels a load of the saved buffer pool state while in progress. For more information, see [InnoDB cache warming for MySQL on Amazon RDS \(p. 1313\)](#).

Syntax

```
CALL mysql.rds_innodb_buffer_pool_load_abort();
```

Usage notes

The master user must run the `mysql.rds_innodb_buffer_pool_load_abort` procedure.

mysql.rds_set_configuration

Specifies the number of hours to retain binary logs or the number of seconds to delay replication.

Syntax

```
CALL mysql.rds_set_configuration(name,value);
```

Parameters

name

The name of the configuration parameter to set.

value

The value of the configuration parameter.

Usage notes

The `mysql.rds_set_configuration` procedure supports the following configuration parameters:

- [Binlog retention hours \(p. 1459\)](#)
- [Target delay \(p. 1460\)](#)

Binlog retention hours

The `binlog retention hours` parameter is used to specify the number of hours to retain binary log files. Amazon RDS normally purges a binary log as soon as possible, but the binary log might still be required for replication with a MySQL database external to Amazon RDS. The default value of `binlog retention hours` is `NULL`. This default value is interpreted as follows:

- For RDS for MySQL, `NULL` means binary logs are not retained (0 hours).

- For Aurora MySQL, NULL means binary logs are cleaned up lazily. Aurora MySQL binary logs might remain in the system for a certain period, usually not longer than a day.

To specify the number of hours for Amazon RDS to retain binary logs on a DB instance, use the `mysql.rds_set_configuration` stored procedure and specify a period with enough time for replication to occur, as shown in the following example.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

For MySQL DB instances, the maximum `binlog retention hours` value is 168 (7 days).

After you set the retention period, monitor storage usage for the DB instance to make sure that the retained binary logs don't take up too much storage.

Target delay

Use the `target_delay` parameter to specify the number of seconds to delay replication from source database instance to the read replica. The specified delay applies to new replicas created from the current DB instance. Amazon RDS normally replicates changes as soon as possible, but some environments might want to delay replication. For example, when replication is delayed, you can roll forward a delayed read replica to the time just before a disaster. If a table is dropped accidentally, you can use delayed replication to recover it quickly. The default value of `target_delay` is 0 (don't delay replication).

For disaster recovery, you can use this configuration parameter with the [mysql.rds_start_replication_until \(p. 1452\)](#) stored procedure or the [mysql.rds_start_replication_until_gtid \(p. 1453\)](#) stored procedure. To roll forward changes to a delayed read replica to the time just before a disaster, you can run the `mysql.rds_set_configuration` procedure with this parameter set. After the `mysql.rds_start_replication_until` or `mysql.rds_start_replication_until_gtid` procedure stops replication, you can promote the read replica to be the new primary DB instance by using the instructions in [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

To use the `mysql.rds_start_replication_until_gtid` procedure, GTID-based replication must be enabled. To skip a specific GTID-based transaction that is known to cause disaster, you can use the [mysql.rds_skip_transaction_with_gtid \(p. 1455\)](#) stored procedure. For more information about working with GTID-based replication, see [Using GTID-based replication for Amazon RDS for MySQL \(p. 1401\)](#).

To specify the number of seconds for Amazon RDS to delay replication to a read replica, use the `mysql.rds_set_configuration` stored procedure and specify the number of seconds to delay replication. The following example specifies that replication is delayed by at least one hour (3,600 seconds).

```
call mysql.rds_set_configuration('target delay', 3600);
```

The limit for the `target_delay` parameter is one day (86400 seconds).

Note

The `target_delay` parameter is only supported for RDS for MySQL.

The `target_delay` parameter isn't supported for RDS for MySQL version 8.0.

mysql.rds_show_configuration

The number of hours that binary logs are retained.

Syntax

```
CALL mysql.rds_show_configuration;
```

Usage notes

To verify the number of hours that Amazon RDS retains binary logs, use the `mysql.rds_show_configuration` stored procedure.

Examples

The following example displays the retention period:

```
call mysql.rds_show_configuration;
      name          value   description
      binlog retention hours    24      binlog retention hours specifies the
duration in hours before binary logs are automatically deleted.
```

mysql.rds_kill

Ends a connection to the MySQL server.

Syntax

```
CALL mysql.rds_kill(processID);
```

Parameters

processID

The identity of the connection thread to be ended.

Usage notes

Each connection to the MySQL server runs in a separate thread. To end a connection, use the `mysql.rds_kill` procedure and pass in the thread ID of that connection. To obtain the thread ID, use the MySQL [SHOW PROCESSLIST](#) command.

Examples

The following example ends a connection with a thread ID of 4243:

```
call mysql.rds_kill(4243);
```

mysql.rds_kill_query

Ends a query running against the MySQL server.

Syntax

```
CALL mysql.rds_kill_query(queryID);
```

Parameters

queryID

The identity of the query to be ended.

Usage notes

To stop a query running against the MySQL server, use the `mysql_rds_kill_query` procedure and pass in the ID of that query. To obtain the query ID, query the MySQL [INFORMATION_SCHEMA PROCESSLIST table](#). The connection to the MySQL server is retained.

Examples

The following example stops a query with a thread ID of 230040:

```
call mysql.rds_kill_query(230040);
```

mysql.rds_rotate_general_log

Rotates the `mysql.general_log` table to a backup table. For more information, see [MySQL database log files \(p. 700\)](#).

Syntax

```
CALL mysql.rds_rotate_general_log;
```

Usage notes

You can rotate the `mysql.general_log` table to a backup table by calling the `mysql.rds_rotate_general_log` procedure. When log tables are rotated, the current log table is copied to a backup log table and the entries in the current log table are removed. If a backup log table already exists, then it is deleted before the current log table is copied to the backup. You can query the backup log table if needed. The backup log table for the `mysql.general_log` table is named `mysql.general_log_backup`.

You can run this procedure only when the `log_output` parameter is set to TABLE.

mysql.rds_rotate_slow_log

Rotates the `mysql.slow_log` table to a backup table. For more information, see [MySQL database log files \(p. 700\)](#).

Syntax

```
CALL mysql.rds_rotate_slow_log;
```

Usage notes

You can rotate the mysql.slow_log table to a backup table by calling the mysql.rds_rotate_slow_log procedure. When log tables are rotated, the current log table is copied to a backup log table and the entries in the current log table are removed. If a backup log table already exists, then it is deleted before the current log table is copied to the backup.

You can query the backup log table if needed. The backup log table for the mysql.slow_log table is named mysql.slow_log_backup.

mysql.rds_enable_gsh_collector

Enables the Global Status History (GoSH) to take default snapshots at intervals specified by rds_set_gsh_collector. For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_enable_gsh_collector;
```

mysql.rds_set_gsh_collector

Specifies the interval, in minutes, between snapshots taken by the Global Status History (GoSH). Default value is For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_set_gsh_collector(intervalPeriod);
```

Parameters

intervalPeriod

The interval, in minutes, between snapshots. Default value is

mysql.rds_disable_gsh_collector

Disables snapshots taken by the Global Status History (GoSH). For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_disable_gsh_collector;
```

mysql.rds_collect_global_status_history

Takes a snapshot on demand for the Global Status History (GoSH). For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_collect_global_status_history;
```

mysql.rds_enable_gsh_rotation

Enables rotation of the contents of the `mysql.global_status_history` table to `mysql.global_status_history_old` at intervals specified by `rds_set_gsh_rotation`. For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_enable_gsh_rotation;
```

mysql.rds_set_gsh_rotation

Specifies the interval, in days, between rotations of the `mysql.global_status_history` table. Default value is 7. For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_set_gsh_rotation(intervalPeriod);
```

Parameters

intervalPeriod

The interval, in days, between table rotations. Default value is 7.

mysql.rds_disable_gsh_rotation

Disables rotation of the `mysql.global_status_history` table. For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_disable_gsh_rotation;
```

mysql.rds_rotate_global_status_history

Rotates the contents of the `mysql.global_status_history` table to `mysql.global_status_history_old` on demand. For more information, see [Managing the global status history \(p. 1431\)](#).

Syntax

```
CALL mysql.rds_rotate_global_status_history;
```

Amazon RDS for Oracle

Amazon RDS supports DB instances that run the following versions and editions of Oracle Database:

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)

Note

Oracle Database 11g, Oracle Database 12c, and Oracle Database 18c are legacy versions that are no longer supported in Amazon RDS.

Before creating a DB instance, complete the steps in the [Setting up for Amazon RDS \(p. 148\)](#) section of this guide. When you create a DB instance using your master account, the account gets DBA privileges, with some limitations. Use this account for administrative tasks such as creating additional database accounts. You can't use SYS, SYSTEM, or other Oracle-supplied administrative accounts.

You can create the following:

- DB instances
- DB snapshots
- Point-in-time restores
- Automated backups
- Manual backups

You can use DB instances running Oracle inside a VPC. You can also add features to your Oracle DB instance by enabling various options. Amazon RDS supports Multi-AZ deployments for Oracle as a high-availability, failover solution.

Important

To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. It also restricts access to certain system procedures and tables that need advanced privileges. You can access your database using standard SQL clients such as Oracle SQL*Plus. However, you can't access the host directly by using Telnet or Secure Shell (SSH).

Topics

- [Overview of Oracle on Amazon RDS \(p. 1467\)](#)
- [Connecting to your Oracle DB instance \(p. 1488\)](#)
- [Securing Oracle DB instance connections \(p. 1498\)](#)
- [Administering your Oracle DB instance \(p. 1521\)](#)
- [Configuring advanced RDS for Oracle features \(p. 1604\)](#)
- [Importing data into Oracle on Amazon RDS \(p. 1615\)](#)
- [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#)
- [Adding options to Oracle DB instances \(p. 1646\)](#)
- [Upgrading the RDS for Oracle DB engine \(p. 1757\)](#)
- [Using third-party software with your RDS for Oracle DB instance \(p. 1766\)](#)

- [Oracle Database engine release notes \(p. 1797\)](#)

Overview of Oracle on Amazon RDS

The following video is a useful introduction to running a production workload on RDS for Oracle.

Topics

- [RDS for Oracle features \(p. 1467\)](#)
- [RDS for Oracle releases \(p. 1470\)](#)
- [RDS for Oracle licensing options \(p. 1474\)](#)
- [RDS for Oracle instance classes \(p. 1477\)](#)
- [RDS for Oracle architecture \(p. 1480\)](#)
- [RDS for Oracle parameters \(p. 1482\)](#)
- [RDS for Oracle character sets \(p. 1482\)](#)
- [RDS for Oracle limitations \(p. 1485\)](#)

RDS for Oracle features

Amazon RDS for Oracle supports most of the features and capabilities of Oracle Database. Some features might have limited support or restricted privileges. Some features are only available in Enterprise Edition, and some require additional licenses. For more information about Oracle Database features for specific Oracle Database versions, see the *Oracle Database Licensing Information User Manual* for the version you're using.

You can filter new Amazon RDS features on the [What's New with Database?](#) page. For **Products**, choose **Amazon RDS**. Then search using keywords such as **Oracle 2022**.

Note

The following lists are not exhaustive.

Topics

- [New features in RDS for Oracle \(p. 1467\)](#)
- [Supported features in RDS for Oracle \(p. 1467\)](#)
- [Unsupported features in RDS for Oracle \(p. 1469\)](#)

New features in RDS for Oracle

To see new RDS for Oracle features, use the following techniques:

- Search [Document history \(p. 2157\)](#) for the keyword **Oracle**.
- You can filter new Amazon RDS features on the [What's New with Database?](#) page. For **Products**, choose **Amazon RDS**. Then search for **Oracle YYYY**, where **YYYY** is a year such as **2022**.

The following video shows a recent video from re:Invent about Oracle new features.

Supported features in RDS for Oracle

Amazon RDS for Oracle supports the following Oracle Database features:

- Advanced Compression
- Application Express (APEX)

For more information, see [Oracle Application Express \(APEX\) \(p. 1664\)](#).

- Automatic Memory Management
- Automatic Undo Management
- Automatic Workload Repository (AWR)

For more information, see [Generating performance reports with Automatic Workload Repository \(AWR\) \(p. 1549\)](#).

- Active Data Guard with Maximum Performance in the same AWS Region or across AWS Regions

For more information, see [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#).

- Blockchain tables (Oracle Database 21c and higher)

For more information, see [Managing Blockchain Tables](#) in the Oracle Database documentation.

- Continuous Query Notification (version 12.1.0.2.v7 and higher)

For more information, see [Using Continuous Query Notification \(CQN\) in the Oracle documentation](#).

- Data Redaction
- Database Change Notification

For more information, see [Database Change Notification](#) in the Oracle documentation.

Note

This feature changes to Continuous Query Notification in Oracle Database 12c Release 1 (12.1) and higher.

- Database In-Memory (Oracle Database 12c and higher)
- Distributed Queries and Transactions
- Edition-Based Redefinition

For more information, see [Setting the default edition for a DB instance \(p. 1553\)](#).

- EM Express (12c and higher)

For more information, see [Oracle Enterprise Manager \(p. 1688\)](#).

- Fine-Grained Auditing
- Flashback Table, Flashback Query, Flashback Transaction Query
- Gradual password rollover for applications (Oracle Database 21c and higher)

For more information, see [Managing Gradual Database Password Rollover for Applications](#) in the Oracle Database documentation.

- HugePages

For more information, see [Turning on HugePages for an RDS for Oracle instance \(p. 1610\)](#).

- Import/export (legacy and Data Pump) and SQL*Loader

For more information, see [Importing data into Oracle on Amazon RDS \(p. 1615\)](#).

- Java Virtual Machine (JVM)

For more information, see [Oracle Java virtual machine \(p. 1685\)](#).

- JavaScript (Oracle Database 21c and higher)

For more information, see [DBMS_MLE](#) in the Oracle Database documentation.

- Label Security (Oracle Database 12c and higher)

For more information, see [Oracle Label Security \(p. 1703\)](#).

- Locator

For more information, see [Oracle Locator \(p. 1706\)](#).

- Materialized Views
- Multimedia

For more information, see [Oracle Multimedia \(p. 1709\)](#).

- Multitenant (single-tenant architecture only)

This feature is available for all Oracle Database 19c and higher releases. For more information, see [RDS for Oracle architecture \(p. 1480\)](#) and [Limitations of a single-tenant CDB \(p. 1486\)](#).

- Network encryption

For more information, see [Oracle native network encryption \(p. 1711\)](#) and [Oracle Secure Sockets Layer \(p. 1722\)](#).

- Partitioning
- Sharding
- Spatial and Graph

For more information, see [Oracle Spatial \(p. 1730\)](#).

- Star Query Optimization
- Streams and Advanced Queuing
- Summary Management – Materialized View Query Rewrite
- Text (File and URL data store types are not supported)
- Total Recall
- Transparent Data Encryption (TDE)

For more information, see [Oracle Transparent Data Encryption \(p. 1751\)](#).

- Unified Auditing, Mixed Mode

For more information, see [Mixed mode auditing](#) in the Oracle documentation.

- XML DB (without the XML DB Protocol Server)

For more information, see [Oracle XML DB \(p. 1756\)](#).

- Virtual Private Database

Unsupported features in RDS for Oracle

Amazon RDS for Oracle doesn't support the following Oracle Database features:

- Automatic Storage Management (ASM)
- Database Vault
- Flashback Database
- FTP and SFTP
- Hybrid partitioned tables
- Messaging Gateway

- Oracle Enterprise Manager Cloud Control Management Repository
- Real Application Clusters (Oracle RAC)
- Real Application Testing
- Unified Auditing, Pure Mode
- Workspace Manager (WMSYS) schema

Note

The preceding list is not exhaustive.

Warning

In general, Amazon RDS doesn't prevent you from creating schemas for unsupported features. However, if you create schemas for Oracle features and components that require SYSDBA privileges, you can damage the data dictionary and affect the availability of your DB instance. Use only supported features and schemas that are available in [Adding options to Oracle DB instances \(p. 1646\)](#).

RDS for Oracle releases

Amazon RDS for Oracle supports multiple Oracle Database releases.

Note

For information about upgrading your releases, see [Upgrading the RDS for Oracle DB engine \(p. 1757\)](#).

Topics

- [Oracle Database 21c with Amazon RDS \(p. 1470\)](#)
- [Oracle Database 19c with Amazon RDS \(p. 1472\)](#)
- [Oracle Database 12c with Amazon RDS \(p. 1473\)](#)

Oracle Database 21c with Amazon RDS

Amazon RDS supports Oracle Database 21c, which includes Oracle Enterprise Edition and Oracle Standard Edition Two. Oracle Database 21c (21.0.0.0) includes many new features and updates from the previous version. A key change is that Oracle Database 21c supports only the multitenant architecture: you can no longer create a database as a traditional non-CDB. To learn more about the differences between CDBs and non-CDBs, see [Limitations of a single-tenant CDB \(p. 1486\)](#).

In this section, you can find the features and changes important to using Oracle Database 21c (21.0.0.0) on Amazon RDS. For a complete list of the changes, see the [Oracle database 21c](#) documentation. For a complete list of features supported by each Oracle Database 21c edition, see [Permitted features, options, and management packs by Oracle database offering](#) in the Oracle documentation.

Amazon RDS parameter changes for Oracle Database 21c (21.0.0.0)

Oracle Database 21c (21.0.0.0) includes several new parameters and parameters with new ranges and new default values.

Topics

- [New parameters \(p. 1471\)](#)
- [Changes for the compatible parameter \(p. 1472\)](#)
- [Removed parameters \(p. 1472\)](#)

New parameters

The following table shows the new Amazon RDS parameters for Oracle Database 21c (21.0.0.0).

Name	Range of values	Default value	Modifiab	Description
blockchain_table_max_no_drop	NONE 0	NONE	Y	Lets you control the maximum amount of idle time that can be specified when creating a blockchain table.
dbnest_enable	NONE CDB_RESOURCE_PDB_ALL	NONE	N	Allows you to enable or disable dbNest. DbNest provides operating system resource isolation and management, file system isolation, and secure computing for PDBs.
dbnest_pdb_fs_conf	NONE <i>pathname</i>	NONE	N	Specifies the dbNest file system configuration file for a PDB.
diagnostics_control	ERROR WARNING IGNORE	IGNORE	Y	Allows you to control and monitor the users who perform potentially unsafe database diagnostic operations.
drpc_dedicated_opt	YES NO	YES	Y	Enables or disables the use of dedicated optimization with Database Resident Connection Pooling (DRCP).
enable_per_pdb_drpc	true false	true	N	Controls whether Database Resident Connection Pooling (DRCP) configures one connection pool for the entire CDB or one isolated connection pool for each PDB.
inmemory_deep_vectorization	true false	true	Y	Enables or disables the deep vectorization framework.
mandatory_user_profile	<i>profile_name</i>	N/A	N	Specifies the mandatory user profile for a CDB or PDB.
optimizer_capture_sql_quarantine	true false	false	Y	Enables or disables the deep vectorization framework.
optimizer_use_sql_quarantine	true false	false	Y	Enables or disables the automatic creation of SQL Quarantine configurations.
result_cache_execution_threshold	0 to 68719476736	2	Y	Specifies the maximum number of times a PL/SQL function can be executed before its result is stored in the result cache.
result_cache_max_temp_result_size	0 to 100	5	Y	Specifies the percentage of RESULT_CACHE_MAX_TEMP_SIZE that any single cached query result can consume.

Name	Range of values	Default value	Modifiable	Description
result_cache_max_temp_size	0 to 2199023255552	RESULT_CACHE_SIZE * 10		Specifies the maximum amount of temporary tablespace (in bytes) that can be consumed by the result cache.
sga_min_size	0 to 2199023255552 (maximum value is 50% of sga_target)	0	Y	Indicates a possible minimum value for SGA usage of a pluggable database (PDB).
tablespace_encryption_default	3DES168 SEED128 ARIA256 ARIA192 ARIA128 3DES168 AES256 AES192 AES128	AES128	Y	Specifies the default algorithm the database uses when encrypting a tablespace.

Changes for the compatible parameter

The compatible parameter has a new maximum value for Oracle Database 21c (21.0.0.0) on Amazon RDS. The following table shows the new default value.

Parameter name	Oracle Database 21c (21.0.0.0) maximum value
compatible	21.0.0

Removed parameters

The following parameters were removed in Oracle Database 21c (21.0.0.0):

- `remote_os_authent`
- `sec_case_sensitive_logon`
- `unified_audit_sga_queue_size`

Oracle Database 19c with Amazon RDS

Amazon RDS supports Oracle Database 19c, which includes Oracle Enterprise Edition and Oracle Standard Edition Two.

Oracle Database 19c (19.0.0.0) includes many new features and updates from the previous version. In this section, you can find the features and changes important to using Oracle Database 19c (19.0.0.0) on Amazon RDS. For a complete list of the changes, see the [Oracle database 19c](#) documentation. For a complete list of features supported by each Oracle Database 19c edition, see [Permitted features, options, and management packs by Oracle database offering](#) in the Oracle documentation.

Amazon RDS parameter changes for Oracle Database 19c (19.0.0.0)

Oracle Database 19c (19.0.0.0) includes several new parameters and parameters with new ranges and new default values.

Topics

- [New parameters \(p. 1473\)](#)
- [Changes to the compatible parameter \(p. 1473\)](#)
- [Removed parameters \(p. 1473\)](#)

New parameters

The following table shows the new Amazon RDS parameters for Oracle Database 19c (19.0.0.0).

Name	Values	Modifi.	Description
lob_signature_enable	TRUE, FALSE (default)	Y	Enables or disables the LOB locator signature feature.
max_datapump_parallel_per_job	1 to 1024, or AUTO	Y	Specifies the maximum number of parallel processes allowed for each Oracle Data Pump job.

Changes to the compatible parameter

The compatible parameter has a new maximum value for Oracle Database 19c (19.0.0.0) on Amazon RDS. The following table shows the new default value.

Parameter name	Oracle Database 19c (19.0.0.0) maximum value
compatible	19.0.0

Removed parameters

The following parameters were removed in Oracle Database 19c (19.0.0.0):

- exafusion_enabled
- max_connections
- o7_dictionary_access

Oracle Database 12c with Amazon RDS

Amazon RDS has deprecated support for Oracle Database 12c on both Oracle Enterprise Edition and Oracle Standard Edition 2.

Topics

- [Oracle Database 12c Release 2 \(12.2.0.1\) with Amazon RDS \(p. 1473\)](#)
- [Oracle Database 12c Release 1 \(12.1.0.2\) with Amazon RDS \(p. 1474\)](#)

Oracle Database 12c Release 2 (12.2.0.1) with Amazon RDS

On March 31, 2022, Oracle Corporation deprecated support for Oracle Database 12c Release 2 (12.2.0.1) for BYOL and LI. On this date, the release moved from Oracle Extended Support to Oracle Sustaining Support, indicating the end of support for this release. For more information, see the end of support timeline on [AWS re:Post](#) and [Oracle Database 12c upgrade considerations \(p. 1762\)](#).

Date	Action
April 1, 2022	Amazon RDS began automatic upgrades of your Oracle Database 12c Release 2 (12.2.0.1) instances to Oracle Database 19c.
April 1, 2022	Amazon RDS began automatic upgrades to Oracle Database 19c for any Oracle Database 12c Release 2 (12.2.0.1) DB instances restored from snapshots. The automatic upgrade occurs during maintenance windows. If maintenance windows aren't available when the upgrade needs to occur, Amazon RDS upgrades the engine immediately.

Oracle Database 12c Release 1 (12.1.0.2) with Amazon RDS

On July 31, 2022, Amazon RDS deprecated support for Oracle Database 12c Release 1 (12.1.0.2) for BYOL and LI. The release moved from Oracle Extended Support to Oracle Sustaining Support, indicating that Oracle Support will no longer release critical patch updates for this release. For more information, see the end of support timeline on [AWS re:Post](#) and [Oracle Database 12c upgrade considerations \(p. 1762\)](#).

Date	Action
August 1, 2022	Amazon RDS began automatic upgrades of your Oracle Database 12c Release 1 (12.1.0.2) instances to the latest Release Update (RU) for Oracle Database 19c. The automatic upgrade occurs during maintenance windows. If maintenance windows aren't available when the upgrade needs to occur, Amazon RDS upgrades the engine immediately.
August 1, 2022	Amazon RDS began automatic upgrades to Oracle Database 19c for any Oracle Database 12c Release 1 (12.1.0.2) DB instances restored from snapshots.

RDS for Oracle licensing options

Amazon RDS for Oracle has two licensing options: License Included (LI) and Bring Your Own License (BYOL). After you create an Oracle DB instance on Amazon RDS, you can change the licensing model by modifying the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

License Included

In the License Included model, you don't need to purchase Oracle Database licenses separately. AWS holds the license for the Oracle database software. In this model, if you have an AWS Support account with case support, contact AWS Support for both Amazon RDS and Oracle Database service requests. The License Included model is only supported on Amazon RDS for Oracle Database Standard Edition Two (SE2).

Bring Your Own License (BYOL)

In the BYOL model, you can use your existing Oracle Database licenses to deploy databases on Amazon RDS. Make sure that you have the appropriate Oracle Database license (with Software Update License and Support) for the DB instance class and Oracle Database edition you wish to run. You must also follow Oracle's policies for licensing Oracle Database software in the cloud computing environment. For more information on Oracle's licensing policy for Amazon EC2, see [Licensing Oracle software in the cloud computing environment](#).

In this model, you continue to use your active Oracle support account, and you contact Oracle directly for Oracle Database service requests. If you have an AWS Support account with case support, you can contact AWS Support for Amazon RDS issues. Amazon Web Services and Oracle have a multi-vendor support process for cases that require assistance from both organizations.

Amazon RDS supports the BYOL model only for Oracle Database Enterprise Edition (EE) and Oracle Database Standard Edition Two (SE2).

Integrating with AWS License Manager

To make it easier to monitor Oracle license usage in the BYOL model, [AWS License Manager](#) integrates with Amazon RDS for Oracle. License Manager supports tracking of RDS for Oracle engine editions and licensing packs based on virtual cores (vCPUs). You can also use License Manager with AWS Organizations to manage all of your organizational accounts centrally.

The following table shows the product information filters for RDS for Oracle.

Filter	Name	Description
Engine Edition	oracle-ee	Oracle Database Enterprise Edition (EE)
	oracle-se2	Oracle Database Standard Edition Two (SE2)
License Pack	data_guard	See Working with read replicas for Amazon RDS for Oracle (p. 1630) (Oracle Active Data Guard)
	olap	See Oracle OLAP (p. 1719)
	ols	See Oracle Label Security (p. 1703)
	diagnostic pack sqlt	See Oracle SQLT (p. 1733)
	tuning pack sqlt	See Oracle SQLT (p. 1733)

To track license usage of your Oracle DB instances, you can create a license configuration. In this case, RDS for Oracle resources that match the product information filter are automatically associated with the license configuration. Discovery of Oracle DB instances can take up to 24 hours.

Console

To create a license configuration to track the license usage of your Oracle DB instances

1. Go to <https://console.aws.amazon.com/license-manager/>.
2. Create a license configuration.

For instructions, see [Create a license configuration](#) in the *AWS License Manager User Guide*.

Add a rule for an **RDS Product Information Filter** in the **Product Information** panel.

For more information, see [ProductInformation](#) in the *AWS License Manager API Reference*.

AWS CLI

To create a license configuration by using the AWS CLI, call the [create-license-configuration](#) command. Use the `--cli-input-json` or `--cli-input-yaml` parameters to pass the parameters to the command.

Example

The following code creates a license configuration for Oracle Enterprise Edition.

```
aws license-manager create-license-configuration --cli-input-json file://rds-oracle-ee.json
```

The following is the sample `rds-oracle-ee.json` file used in the example.

```
{
    "Name": "rds-oracle-ee",
    "Description": "RDS Oracle Enterprise Edition",
    "LicenseCountingType": "vCPU",
    "LicenseCountHardLimit": false,
    "ProductInformationList": [
        {
            "ResourceType": "RDS",
            "ProductInformationFilterList": [
                {
                    "ProductInformationFilterName": "Engine Edition",
                    "ProductInformationFilterValue": ["oracle-ee"],
                    "ProductInformationFilterComparator": "EQUALS"
                }
            ]
        }
    ]
}
```

For more information about product information, see [Automated discovery of resource inventory](#) in the *AWS License Manager User Guide*.

For more information about the `--cli-input` parameter, see [Generating AWS CLI skeleton and input parameters from a JSON or YAML input file](#) in the *AWS CLI User Guide*.

Migrating between Oracle editions

If you have an unused BYOL Oracle license appropriate for the edition and class of DB instance that you plan to run, you can migrate from Standard Edition 2 (SE2) to Enterprise Edition (EE). You can't migrate from Enterprise Edition to other editions.

To change the edition and retain your data

1. Create a snapshot of the DB instance.

For more information, see [Creating a DB snapshot \(p. 448\)](#).

2. Restore the snapshot to a new DB instance, and select the Oracle database edition you want to use.

For more information, see [Restoring from a DB snapshot \(p. 452\)](#).

3. (Optional) Delete the old DB instance, unless you want to keep it running and have the appropriate Oracle Database licenses for it.

For more information, see [Deleting a DB instance \(p. 421\)](#).

Licensing Oracle Multi-AZ deployments

Amazon RDS supports Multi-AZ deployments for Oracle as a high-availability, failover solution. We recommend Multi-AZ for production workloads. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

If you use the Bring Your Own License model, you must have a license for both the primary DB instance and the standby DB instance in a Multi-AZ deployment.

RDS for Oracle instance classes

The computation and memory capacity of a DB instance is determined by its instance class. The DB instance class you need depends on your processing power and memory requirements.

Supported RDS for Oracle instance classes

The supported RDS for Oracle instance classes are a subset of the RDS DB instance classes. For the complete list of RDS instance classes, see [DB instance classes \(p. 10\)](#).

RDS for Oracle also offers instance classes that are optimized for workloads that require additional memory, storage, and I/O per vCPU. These instance classes use the following naming convention:

```
db.r5b.instance_size.tpcthreads_per_core.memratio  
db.r5.instance_size.tpcthreads_per_core.memratio
```

The following is an example of a supported instance class:

```
db.r5b.4xlarge.tpc2.mem2x
```

The components of the preceding instance class name are as follows:

- db.r5b.4xlarge – The name of the instance class.
- tpc2 – The threads per core. A value of 2 means that multithreading is turned on. If the value is 1, multithreading is turned off.
- mem2x – The ratio of additional memory to the standard memory for the instance class. In this example, the optimization provides twice as much memory as a standard db.r5.4xlarge instance.

The following table lists all instance classes supported for Oracle Database. Oracle Database 12c Release 1 (12.1.0.2) and Oracle Database 12c Release 2 (12.2.0.2) are listed in the table, but support for these releases is deprecated. For information about the memory attributes of each type, see [RDS for Oracle instance types](#).

Oracle edition	Oracle Database 19c and higher, Oracle Database 12c Release 2 (12.2.0.1) (deprecated)	Oracle Database 12c Release 1 (12.1.0.2) (deprecated)
Enterprise Edition (EE) Bring Your Own License (BYOL)	Standard instance classes db.m6i.large–db.m6i.32xlarge (19c only) db.m5d.large–db.m5d.24xlarge db.m5.large–db.m5.24xlarge db.m4.large–db.m4.16xlarge	db.m5.large–db.m5.24xlarge db.m4.large–db.m4.16xlarge
	Memory optimized instance classes	
	db.r6i.large–db.r6i.32xlarge (19c only) db.r5d.large–db.r5d.24xlarge	db.r5.12xlarge.tpc2.mem2x db.r5b.large–db.r5b.24xlarge

Oracle edition	Oracle Database 19c and higher, Oracle Database 12c Release 2 (12.2.0.1) (deprecated)	Oracle Database 12c Release 1 (12.1.0.2) (deprecated)
	db.r5b.8xlarge(tpc2.mem3x) db.r5b.6xlarge(tpc2.mem4x) db.r5b.4xlarge(tpc2.mem4x) db.r5b.4xlarge(tpc2.mem3x) db.r5b.4xlarge(tpc2.mem2x) db.r5b.2xlarge(tpc2.mem8x) db.r5b.2xlarge(tpc2.mem4x) db.r5b.2xlarge(tpc1.mem2x) db.r5b.xlarge(tpc2.mem4x) db.r5b.xlarge(tpc2.mem2x) db.r5b.large(tpc1.mem2x) db.r5b.large-db.r5b.24xlarge db.r5.12xlarge(tpc2.mem2x) db.r5.8xlarge(tpc2.mem3x) db.r5.6xlarge(tpc2.mem4x) db.r5.4xlarge(tpc2.mem4x) db.r5.4xlarge(tpc2.mem3x) db.r5.4xlarge(tpc2.mem2x) db.r5.2xlarge(tpc2.mem8x) db.r5.2xlarge(tpc2.mem4x) db.r5.2xlarge(tpc1.mem2x) db.r5.xlarge(tpc2.mem4x) db.r5.xlarge(tpc2.mem2x) db.r5.large(tpc1.mem2x) db.r5.large-db.r5.24xlarge db.r4.large-db.r4.16xlarge db.x1e.xlarge-db.x1e.32xlarge db.x1.16xlarge-db.x1.32xlarge db.z1d.large-db.z1d.12xlarge	db.r5.8xlarge(tpc2.mem3x) db.r5.6xlarge(tpc2.mem4x) db.r5.4xlarge(tpc2.mem4x) db.r5.4xlarge(tpc2.mem3x) db.r5.4xlarge(tpc2.mem2x) db.r5.2xlarge(tpc2.mem8x) db.r5.2xlarge(tpc2.mem4x) db.r5.2xlarge(tpc1.mem2x) db.r5.xlarge(tpc2.mem4x) db.r5.xlarge(tpc2.mem2x) db.r5.large-db.r5.24xlarge db.r4.large-db.r4.16xlarge db.x1e.xlarge-db.x1e.32xlarge db.x1.16xlarge-db.x1.32xlarge db.z1d.large-db.z1d.12xlarge

Oracle edition	Oracle Database 19c and higher, Oracle Database 12c Release 2 (12.2.0.1) (deprecated)	Oracle Database 12c Release 1 (12.1.0.2) (deprecated)
	Burstable performance instance classes	
	db.t3.small–db.t3.2xlarge	db.t3.micro–db.t3.2xlarge
Standard Edition 2 (SE2) Bring Your Own License (BYOL)	Standard instance classes	
	db.m6i.large–db.m6i.4xlarge (19c only)	db.m5.large–db.m5.4xlarge
	db.m5d.large–db.m5d.4xlarge	db.m4.large–db.m4.4xlarge
	db.m5.large–db.m5.4xlarge	
	db.m4.large–db.m4.4xlarge	
	Memory optimized instance classes	
	db.r6i.large–db.r6i.4xlarge (19c only)	db.r5.4xlarge.tpc2.mem4x
	db.r5d.large–db.r5d.4xlarge	db.r5.4xlarge.tpc2.mem3x
	db.r5.4xlarge.tpc2.mem4x	db.r5.4xlarge.tpc2.mem2x
	db.r5.4xlarge.tpc2.mem3x	db.r5.2xlarge.tpc2.mem8x
	db.r5.4xlarge.tpc2.mem2x	db.r5.2xlarge.tpc2.mem4x
	db.r5.2xlarge.tpc2.mem8x	db.r5.2xlarge.tpc1.mem2x
	db.r5.2xlarge.tpc2.mem4x	db.r5.xlarge.tpc2.mem4x
	db.r5.2xlarge.tpc1.mem2x	db.r5.xlarge.tpc2.mem2x
	db.r5.xlarge.tpc2.mem4x	db.r5.large.tpc1.mem2x
	db.r5.large.tpc1.mem2x	db.r5.large–db.r5.4xlarge
	db.r5.large–db.r5.4xlarge	db.r4.large–db.r4.4xlarge
	db.r5b.large–db.r5b.4xlarge	db.z1d.large–db.z1d.3xlarge
	db.r4.large–db.r4.4xlarge	
	db.z1d.large–db.z1d.3xlarge	
	Burstable performance instance classes	
	db.t3.small–db.t3.2xlarge	db.t3.micro–db.t3.2xlarge
Standard Edition 2 (SE2) License Included	Standard instance classes	
	db.m5.large–db.m5.4xlarge	db.m5.large–db.m5.4xlarge
	db.m4.large–db.m4.4xlarge	db.m4.large–db.m4.4xlarge
	Memory optimized instance classes	

Oracle edition	Oracle Database 19c and higher, Oracle Database 12c Release 2 (12.2.0.1) (deprecated)	Oracle Database 12c Release 1 (12.1.0.2) (deprecated)
	db.r5.large-db.r5.4xlarge db.r4.large-db.r4.4xlarge	db.r5.large-db.r5.4xlarge db.r4.large-db.r4.4xlarge
	Burstable performance instance classes	
	db.t3.small-db.t3.2xlarge	db.t3.micro-db.t3.2xlarge

Note

We encourage all BYOL customers to consult their licensing agreement to assess the impact of Amazon RDS for Oracle deprecations. For more information on the compute capacity of DB instance classes supported by RDS for Oracle, see [DB instance classes \(p. 10\)](#) and [Configuring the processor for a DB instance class \(p. 42\)](#).

Note

If you have DB snapshots of DB instances that were using deprecated DB instance classes, you can choose a DB instance class that is not deprecated when you restore the DB snapshots. For more information, see [Restoring from a DB snapshot \(p. 452\)](#).

Deprecated Oracle DB instance classes

The following DB instance classes are deprecated for RDS for Oracle:

- db.m1, db.m2, db.m3
- db.t3.micro (supported only on 12.1.0.2, which is deprecated)
- db.t1, db.t2
- db.r1, db.r2, db.r3

The preceding DB instance classes have been replaced by better performing DB instance classes that are generally available at a lower cost. RDS for Oracle automatically scales DB instances to DB instance classes that are not deprecated.

If you have DB instances that use deprecated DB instance classes, Amazon RDS will modify each one automatically to use a comparable DB instance class that is not deprecated. You can change the DB instance class for a DB instance yourself by modifying the DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

If you have DB snapshots of DB instances that were using deprecated DB instance classes, you can choose a DB instance class that is not deprecated when you restore the DB snapshots. For more information, see [Restoring from a DB snapshot \(p. 452\)](#).

RDS for Oracle architecture

The *multitenant architecture* enables an Oracle database to function as a *multitenant container database (CDB)*. A CDB can include customer-created *pluggable databases (PDBs)*. A *non-CDB* is an Oracle database that uses the traditional architecture, which can't contain PDBs. For more information about the multitenant architecture, see [Oracle Multitenant Administrator's Guide](#).

The architecture is a permanent characteristic that you can't change later. The architecture requirements are as follows:

Oracle Database 21c

You must create the instance as a CDB.

Oracle Database 19c

You can create the instance as either a CDB or non-CDB.

Oracle Database 12c

You must create the instance as a non-CDB.

For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Currently, Amazon RDS supports a subset of multitenant architecture called the *single-tenant architecture*. In this case, your CDB contains only one PDB. The single-tenant architecture uses the same RDS APIs as the non-CDB architecture. Your experience with a non-CDB is mostly identical to your experience with a PDB. You can't access the CDB itself.

The following sections explain the principal differences between the non-multitenant and single-tenant architectures. For more information, see [Limitations of a single-tenant CDB \(p. 1486\)](#).

Topics

- [Database creation and connections in a single-tenant architecture \(p. 1481\)](#)
- [Database upgrades in a single-tenant architecture \(p. 1481\)](#)
- [User accounts and privileges in a single-tenant architecture \(p. 1481\)](#)
- [Parameters in a single-tenant architecture \(p. 1482\)](#)
- [Snapshots in a single-tenant architecture \(p. 1482\)](#)
- [Data migration in a single-tenant architecture \(p. 1482\)](#)

Database creation and connections in a single-tenant architecture

When you create a CDB, specify the DB instance identifier just as for a non-CDB. The instance identifier forms the first part of your endpoint. The system identifier (SID) is the name of the CDB. The SID of every CDB is RDSCDB. You can't choose a different value.

In the single-tenant architecture, you always connect to the PDB rather than the CDB. Specify the endpoint for the PDB just as for a non-CDB. The only difference is that you specify *pdb_name* for the database name, where *pdb_name* is the name you chose for your PDB. The following example shows the format for the connection string in SQL*Plus.

```
sqlplus 'dbuser@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=endpoint)(PORT=port))(CONNECT_DATA=(SID=pdb_name))'
```

Database upgrades in a single-tenant architecture

You can upgrade a CDB to a different Oracle Database release. For example, you can upgrade a DB instance from Oracle Database 19c to Oracle Database 21c. You can't upgrade a non-CDB to a CDB.

User accounts and privileges in a single-tenant architecture

In the Oracle multitenant architecture, all users accounts are either *common users* or *local users*. A CDB common user is a database user whose single identity and password are known in the CDB root and in every existing and future PDB. In contrast, a local user exists only in a single PDB.

The RDS master user is a local user account in the PDB. If you create new user accounts, these users will also be local users residing in the PDB. You can't use any user accounts to create new PDBs or modify the state of the existing PDB.

The `rdsadmin` user is a common user account. You can run Oracle for RDS packages that exist in this account, but you can't log in as `rdsadmin`. For more information, see [About Common Users and Local Users](#) in the Oracle documentation.

Parameters in a single-tenant architecture

CDBs have their own parameter classes and different default parameter values. The CDB parameter classes are as follows:

- `oracle-ee-cdb-21`
- `oracle-se2-cdb-21`
- `oracle-ee-cdb-19`
- `oracle-se2-cdb-19`

You specify parameters at the CDB level rather than the PDB level. The PDB inherits parameter settings from the CDB. For more information about setting parameters, see [Working with DB parameter groups \(p. 227\)](#).

Snapshots in a single-tenant architecture

Snapshots work the same in a single-tenant and non-multitenant architecture. The only difference is that when you restore a snapshot, you can only rename the PDB, not the CDB. The CDB is always named RDSCDB. For more information, see [Oracle Database considerations \(p. 454\)](#).

Data migration in a single-tenant architecture

RDS for Oracle doesn't support unplugging and plugging in PDBs. For more information about migrating data, see [Importing data into Oracle on Amazon RDS \(p. 1615\)](#).

RDS for Oracle parameters

In Amazon RDS, you manage parameters using parameter groups. For more information, see [Working with parameter groups \(p. 289\)](#). To view the supported parameters for a specific Oracle Database edition and version, run the AWS CLI command `describe-engine-default-parameters`.

For example, to view the supported parameters for the Enterprise Edition of Oracle Database 19c, run the following command.

```
aws rds describe-engine-default-parameters \
--db-parameter-group-family oracle-ee-19
```

RDS for Oracle character sets

RDS for Oracle supports two types of character sets: the DB character set and national character set.

DB character set

The Oracle database character set is used in the CHAR, VARCHAR2, and CL0B data types. The database also uses this character set for metadata such as table names, column names, and SQL statements. The Oracle database character set is typically referred to as the *DB character set*.

You set the character set when you create a DB instance. You can't change the DB character set after you create the database.

Supported DB character sets

The following table lists the Oracle DB character sets that are supported in Amazon RDS. You can use a value from this table with the `--character-set-name` parameter of the AWS CLI [create-db-instance](#) command or with the `CharacterSet` parameter of the Amazon RDS API [CreateDBInstance](#) operation.

Note

The character set for a CDB is always AL32UTF8. You can set a different character set for the PDB only.

Value	Description
AL32UTF8	Unicode 5.0 UTF-8 Universal character set (default)
AR8ISO8859P6	ISO 8859-6 Latin/Arabic
AR8MSWIN1256	Microsoft Windows Code Page 1256 8-bit Latin/Arabic
BLT8ISO8859P13	ISO 8859-13 Baltic
BLT8MSWIN1257	Microsoft Windows Code Page 1257 8-bit Baltic
CL8ISO8859P5	ISO 8859-5 Latin/Cyrillic
CL8MSWIN1251	Microsoft Windows Code Page 1251 8-bit Latin/Cyrillic
EE8ISO8859P2	ISO 8859-2 East European
EL8ISO8859P7	ISO 8859-7 Latin/Greek
EE8MSWIN1250	Microsoft Windows Code Page 1250 8-bit East European
EL8MSWIN1253	Microsoft Windows Code Page 1253 8-bit Latin/Greek
IW8ISO8859P8	ISO 8859-8 Latin/Hebrew
IW8MSWIN1255	Microsoft Windows Code Page 1255 8-bit Latin/Hebrew
JA16EUC	EUC 24-bit Japanese
JA16EUCTILDE	Same as JA16EUC except for mapping of wave dash and tilde to and from Unicode
JA16SJIS	Shift-JIS 16-bit Japanese
JA16SJISTILDE	Same as JA16SJIS except for mapping of wave dash and tilde to and from Unicode
KO16MSWIN949	Microsoft Windows Code Page 949 Korean
NE8ISO8859P10	ISO 8859-10 North European

Value	Description
NEE8ISO8859P4	ISO 8859-4 North and Northeast European
TH8TISASCII	Thai Industrial Standard 620-2533-ASCII 8-bit
TR8MSWIN1254	Microsoft Windows Code Page 1254 8-bit Turkish
US7ASCII	ASCII 7-bit American
UTF8	Unicode 3.0 UTF-8 Universal character set, CESU-8 compliant
VN8MSWIN1258	Microsoft Windows Code Page 1258 8-bit Vietnamese
WE8ISO8859P1	Western European 8-bit ISO 8859 Part 1
WE8ISO8859P15	ISO 8859-15 West European
WE8ISO8859P9	ISO 8859-9 West European and Turkish
WE8MSWIN1252	Microsoft Windows Code Page 1252 8-bit West European
ZHS16GBK	GBK 16-bit Simplified Chinese
ZHT16HKSCS	Microsoft Windows Code Page 950 with Hong Kong Supplementary Character Set HKSCS-2001. Character set conversion is based on Unicode 3.0.
ZHT16MSWIN950	Microsoft Windows Code Page 950 Traditional Chinese
ZHT32EUC	EUC 32-bit Traditional Chinese

NLS_LANG environment variable

A *locale* is a set of information addressing linguistic and cultural requirements that corresponds to a given language and country. Setting the NLS_LANG environment variable in your client's environment is the simplest way to specify locale behavior for Oracle. This variable sets the language and territory used by the client application and the database server. It also indicates the client's character set, which corresponds to the character set for data entered or displayed by a client application. For more information on NLS_LANG and character sets, see [What is a character set or code page?](#) in the Oracle documentation.

NLS initialization parameters

You can also set the following National Language Support (NLS) initialization parameters at the instance level for an Oracle DB instance in Amazon RDS:

- NLS_DATE_FORMAT
- NLS_LENGTH_SEMANTICS
- NLS_NCHAR_CONV_EXCP
- NLS_TIME_FORMAT
- NLS_TIME_TZ_FORMAT
- NLS_TIMESTAMP_FORMAT
- NLS_TIMESTAMP_TZ_FORMAT

For information about modifying instance parameters, see [Working with parameter groups \(p. 289\)](#).

You can set other NLS initialization parameters in your SQL client. For example, the following statement sets the NLS_LANGUAGE initialization parameter to GERMAN in a SQL client that is connected to an Oracle DB instance:

```
ALTER SESSION SET NLS_LANGUAGE=GERMAN;
```

For information about connecting to an Oracle DB instance with a SQL client, see [Connecting to your Oracle DB instance \(p. 1488\)](#).

National character set

The national character set is used in the NCHAR, NVARCHAR2, and NCLOB data types. The national character set is typically referred to as the *NCHAR character set*. Unlike the DB character set, the NCHAR character set doesn't affect database metadata.

The NCHAR character set supports the following character sets:

- AL16UTF16 (default)
- UTF8

You can specify either value with the --nchar-character-set-name parameter of the [create-db-instance](#) command (AWS CLI version 2 only). If you use the Amazon RDS API, specify the NcharCharacterSetName parameter of [CreateDBInstance](#) operation. You can't change the national character set after you create the database.

For more information about Unicode in Oracle databases, see [Supporting multilingual databases with unicode](#) in the Oracle documentation.

RDS for Oracle limitations

Following are important limitations of using RDS for Oracle.

Note

This list is not exhaustive.

Topics

- [Oracle file size limits in Amazon RDS \(p. 1485\)](#)
- [Public synonyms for Oracle-supplied schemas \(p. 1486\)](#)
- [Schemas for unsupported features \(p. 1486\)](#)
- [Limitations for Oracle DBA privileges \(p. 1486\)](#)
- [Limitations of a single-tenant CDB \(p. 1486\)](#)
- [Deprecation of TLS 1.0 and 1.1 Transport Layer Security \(p. 1487\)](#)

Oracle file size limits in Amazon RDS

The maximum size of a single file on RDS for Oracle DB instances is 16 TiB (tebibytes). If you try to resize a data file in a bigfile tablespace to a value over the limit, you receive an error such as the following.

```
ORA-01237: cannot extend datafile 6
ORA-01110: data file 6: '/rdsdbdata/db/mydir/datafile/myfile.dbf'
ORA-27059: could not reduce file size
Linux-x86_64 Error: 27: File too large
```

Additional information: 2

Public synonyms for Oracle-supplied schemas

Don't create or modify public synonyms for Oracle-supplied schemas, including SYS, SYSTEM, and RDSADMIN. Such actions might result in invalidation of core database components and affect the availability of your DB instance.

You can create public synonyms referencing objects in your own schemas.

Schemas for unsupported features

In general, Amazon RDS doesn't prevent you from creating schemas for unsupported features. However, if you create schemas for Oracle features and components that require SYS privileges, you can damage the data dictionary and affect your instance availability. Use only supported features and schemas that are available in [Adding options to Oracle DB instances \(p. 1646\)](#).

Limitations for Oracle DBA privileges

In the database, a *role* is a collection of privileges that you can grant to or revoke from a user. An Oracle database uses roles to provide security.

The predefined role DBA normally allows all administrative privileges on an Oracle database. When you create a DB instance, your master user account gets DBA privileges (with some limitations). To deliver a managed experience, an RDS for Oracle database doesn't provide the following privileges for the DBA role:

- ALTER DATABASE
- ALTER SYSTEM
- CREATE ANY DIRECTORY
- DROP ANY DIRECTORY
- GRANT ANY PRIVILEGE
- GRANT ANY ROLE

Use the master user account for administrative tasks such as creating additional user accounts in the database. You can't use SYS, SYSTEM, and other Oracle-supplied administrative accounts.

Limitations of a single-tenant CDB

The following options aren't supported for the single-tenant architecture:

- Database Activity Streams
- Oracle Data Guard
- Oracle Enterprise Manager
- Oracle Enterprise Manager Agent
- Oracle Label Security

The following operations work in a single-tenant CDB, but no customer-visible mechanism can detect the current status of the operations:

- Enabling and disabling block change tracking (p. 1574)
- Enabling auditing for the SYS.AUD\$ table (p. 1553)

Note

Auditing information isn't available from within the PDB.

Deprecation of TLS 1.0 and 1.1 Transport Layer Security

Transport Layer Security protocol versions 1.0 and 1.1 (TLS 1.0 and TLS 1.1) are deprecated. In accordance with security best practices, Oracle has deprecated the use of TLS 1.0 and TLS 1.1. To meet your security requirements, RDS for Oracle strongly recommends that you use TLS 1.2 instead.

Connecting to your Oracle DB instance

After Amazon RDS provisions your Oracle DB instance, you can use any standard SQL client application to connect to the DB instance. In this topic, you connect to a DB instance that is running the Oracle database engine by using Oracle SQL Developer or SQL*Plus.

For an example that walks you through the process of creating and connecting to a sample DB instance, see [Creating an Oracle DB instance and connecting to a database on an Oracle DB instance \(p. 180\)](#).

Topics

- [Finding the endpoint of your Oracle DB instance \(p. 1488\)](#)
- [Connecting to your DB instance using Oracle SQL developer \(p. 1490\)](#)
- [Connecting to your DB instance using SQL*Plus \(p. 1492\)](#)
- [Considerations for security groups \(p. 1493\)](#)
- [Considerations for process architecture \(p. 1493\)](#)
- [Troubleshooting connections to your Oracle DB instance \(p. 1493\)](#)
- [Modifying connection properties using sqlnet.ora parameters \(p. 1494\)](#)

Finding the endpoint of your Oracle DB instance

Each Amazon RDS DB instance has an endpoint, and each endpoint has the DNS name and port number for the DB instance. To connect to your DB instance using a SQL client application, you need the DNS name and port number for your DB instance.

You can find the endpoint for a DB instance using the Amazon RDS console or the AWS CLI.

Note

If you are using Kerberos authentication, see [Connecting to Oracle with Kerberos authentication \(p. 1512\)](#).

Console

To find the endpoint using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the console, choose the AWS Region of your DB instance.
3. Find the DNS name and port number for your DB Instance.
 - a. Choose **Databases** to display a list of your DB instances.
 - b. Choose the Oracle DB instance name to display the instance details.
 - c. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

database-1

[Modify](#)

Summary

DB identifier database-1	CPU <div style="width: 2.3%; background-color: #ff9999; height: 10px;"></div> 2.30%	Status Available	Class db.m4.large
Role Instance	Current activity <div style="width: 0.01%; background-color: #0070C0; height: 10px;"></div> 0.01 Sessions	Engine Oracle Standard Edition Two	Region & AZ us-east-1f

[Connectivity & security](#) [Monitoring](#) [Logs & events](#) [Configuration](#) [Maintenance & backups](#)

Connectivity & security

Endpoint & port Endpoint database-1. .us-east-1.rds.amazonaws.com Port 1521	Networking Availability zone us-east-1f VPC vpc-1234567f Subnet group	Security VPC security groups default (sg-0a5cba2b) (active) Public accessibility No
--	---	--

AWS CLI

To find the endpoint of an Oracle DB instance by using the AWS CLI, call the [describe-db-instances](#) command.

Example To find the endpoint using the AWS CLI

```
aws rds describe-db-instances
```

Search for Endpoint in the output to find the DNS name and port number for your DB instance. The Address line in the output contains the DNS name. The following is an example of the JSON endpoint output.

```
{"Endpoint": {  
    "HostedZoneId": "Z1PVIF0B656C1W",  
    "Port": 3306,  
    "Address": "myinstance.123456789012.us-west-2.rds.amazonaws.com"  
},
```

Note

The output might contain information for multiple DB instances.

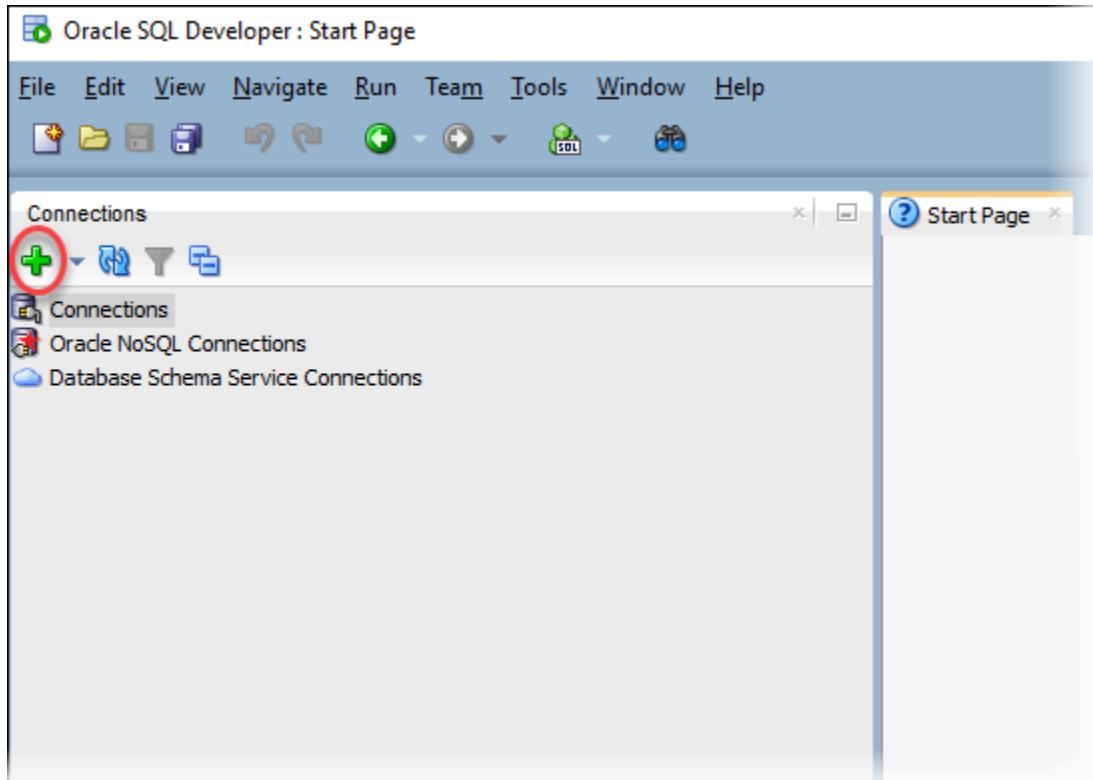
Connecting to your DB instance using Oracle SQL developer

In this procedure, you connect to your DB instance by using Oracle SQL Developer. To download a standalone version of this utility, see the [Oracle SQL developer downloads page](#).

To connect to your DB instance, you need its DNS name and port number. For information about finding the DNS name and port number for a DB instance, see [Finding the endpoint of your Oracle DB instance \(p. 1488\)](#).

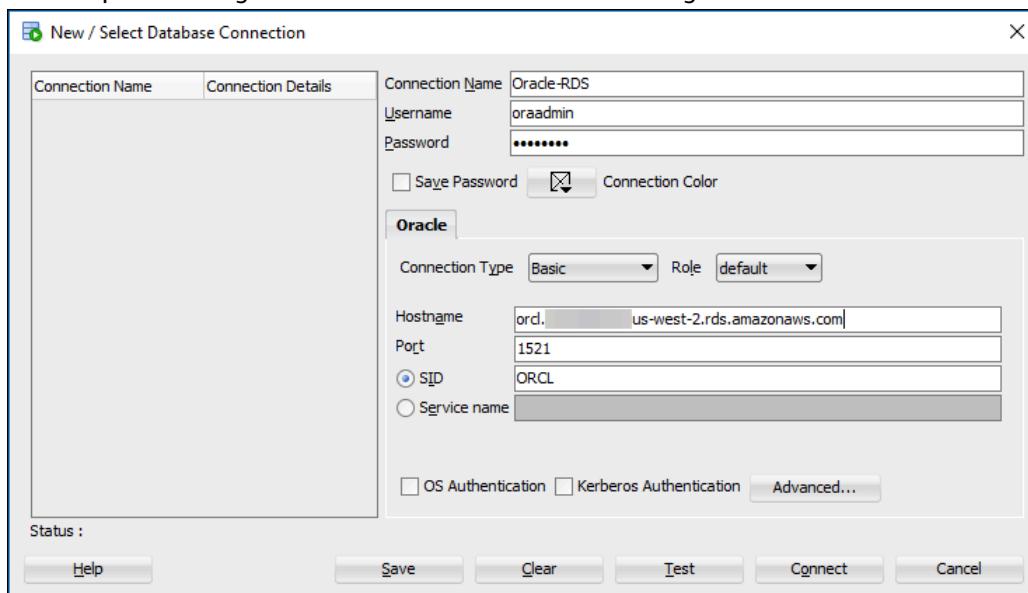
To connect to a DB instance using SQL developer

1. Start Oracle SQL Developer.
2. On the **Connections** tab, choose the **add (+)** icon.



3. In the **New>Select Database Connection** dialog box, provide the information for your DB instance:
 - For **Connection Name**, enter a name that describes the connection, such as Oracle-RDS.
 - For **Username**, enter the name of the database administrator for the DB instance.
 - For **Password**, enter the password for the database administrator.
 - For **Hostname**, enter the DNS name of the DB instance.
 - For **Port**, enter the port number.
 - For **SID**, enter the Oracle database SID.

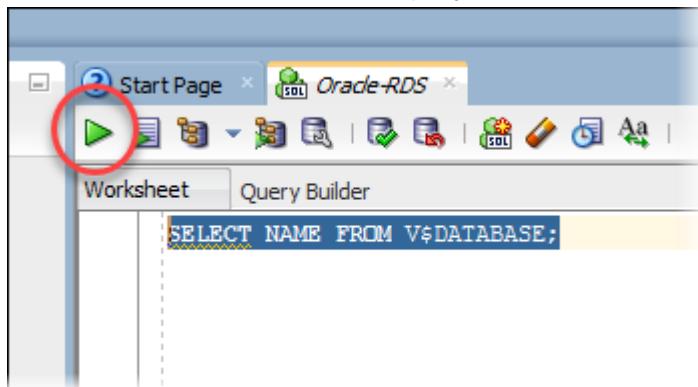
The completed dialog box should look similar to the following.



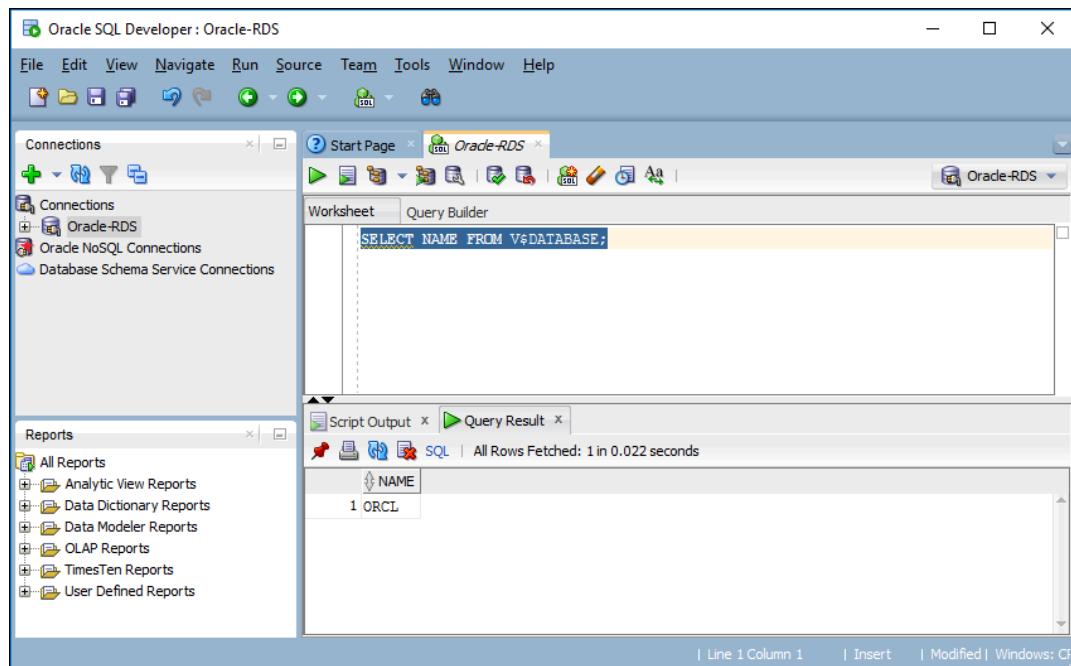
4. Choose **Connect**.
5. You can now start creating your own databases and running queries against your DB instance and databases as usual. To run a test query against your DB instance, do the following:
 - a. In the **Worksheet** tab for your connection, enter the following SQL query.

```
SELECT NAME FROM V$DATABASE;
```

- b. Choose the **execute** icon to run the query.



SQL Developer returns the database name.



Connecting to your DB instance using SQL*Plus

You can use a utility like SQL*Plus to connect to an Amazon RDS DB instance running Oracle. To download Oracle Instant Client, which includes a standalone version of SQL*Plus, see [Oracle Instant Client Downloads](#).

To connect to your DB instance, you need its DNS name and port number. For information about finding the DNS name and port number for a DB instance, see [Finding the endpoint of your Oracle DB instance \(p. 1488\)](#).

Example To connect to an Oracle DB instance using SQL*Plus

In the following examples, substitute the user name of your DB instance administrator. Also, substitute the DNS name for your DB instance, and then include the port number and the Oracle SID. The SID value is the name of the DB instance's database that you specified when you created the DB instance, and not the name of the DB instance.

For Linux, macOS, or Unix:

```
sqlplus 'user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))(CONNECT_DATA=(SID=database_name)))'
```

For Windows:

```
sqlplus user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))(CONNECT_DATA=(SID=database_name)))
```

You should see output similar to the following.

```
SQL*Plus: Release 12.1.0.2.0 Production on Mon Aug 21 09:42:20 2017
```

After you enter the password for the user, the SQL prompt appears.

```
SQL>
```

Note

The shorter format connection string (Easy connect or EZCONNECT), such as `sqlplus USER/PASSWORD@LONGER-THAN-63-CHARS-RDS-ENDPOINT-HERE:1521/DATABASE_IDENTIFIER`, might encounter a maximum character limit and should not be used to connect.

Considerations for security groups

For you to connect to your DB instance, it must be associated with a security group that contains the necessary IP addresses and network configuration. Your DB instance might use the default security group. If you assigned a default, nonconfigured security group when you created the DB instance, the firewall prevents connections. For information about creating a new security group, see [Controlling access with security groups \(p. 2085\)](#).

After you create the new security group, you modify your DB instance to associate it with the security group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

You can enhance security by using SSL to encrypt connections to your DB instance. For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

Considerations for process architecture

Server processes handle user connections to an Oracle DB instance. By default, the Oracle DB instance uses dedicated server processes. With dedicated server processes, each server process services only one user process. You can optionally configure shared server processes. With shared server processes, each server process can service multiple user processes.

You might consider using shared server processes when a high number of user sessions are using too much memory on the server. You might also consider shared server processes when sessions connect and disconnect very often, resulting in performance issues. There are also disadvantages to using shared server processes. For example, they can strain CPU resources, and they are more complicated to configure and administer.

For more information about dedicated and shared server processes, see [About dedicated and shared server processes](#) in the Oracle documentation. For more information about configuring shared server processes on an RDS for Oracle DB instance, see [How do I configure Amazon RDS for Oracle database to work with shared servers?](#) in the Knowledge Center.

Troubleshooting connections to your Oracle DB instance

The following are issues you might encounter when you try to connect to your Oracle DB instance.

Issue	Troubleshooting suggestions
Unable to connect to your DB instance.	For a newly created DB instance, the DB instance has a status of creating until it is ready to use. When the state changes to available ,

Issue	Troubleshooting suggestions
	you can connect to the DB instance. Depending on the DB instance class and the amount of storage, it can take up to 20 minutes before the new DB instance is available.
Unable to connect to your DB instance.	If you can't send or receive communications over the port that you specified when you created the DB instance, you can't connect to the DB instance. Check with your network administrator to verify that the port you specified for your DB instance allows inbound and outbound communication.
Unable to connect to your DB instance.	<p>The access rules enforced by your local firewall and the IP addresses you authorized to access your DB instance in the security group for the DB instance might not match. The problem is most likely the inbound or outbound rules on your firewall.</p> <p>You can add or edit an inbound rule in the security group. For Source, choose My IP. This allows access to the DB instance from the IP address detected in your browser. For more information, see Amazon VPC VPCs and Amazon RDS (p. 2103).</p> <p>For more information about security groups, see Controlling access with security groups (p. 2085).</p> <p>To walk through the process of setting up rules for your security group, see Tutorial: Create a VPC for use with a DB instance (IPv4 only) (p. 2120).</p>
Connect failed because target host or object does not exist – Oracle, Error: ORA-12545	<p>Make sure that you specified the server name and port number correctly. For Server name, enter the DNS name from the console.</p> <p>For information about finding the DNS name and port number for a DB instance, see Finding the endpoint of your Oracle DB instance (p. 1488).</p>
Invalid username/password; logon denied – Oracle, Error: ORA-01017	You were able to reach the DB instance, but the connection was refused. This is usually caused by providing an incorrect user name or password. Verify the user name and password, and then retry.
TNS:listener does not currently know of SID given in connect descriptor – Oracle, ERROR: ORA-12505	Ensure the correct SID is entered. The SID is the same as your DB name. Find the DB name in the Configuration tab of the Databases page for your instance. You can also find the DB name using the AWS CLI: <code>aws rds describe-db-instances --query 'DBInstances[*].[DBInstanceIdentifier,DBName]' --output text</code>

For more information on connection issues, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#).

Modifying connection properties using sqlnet.ora parameters

The sqlnet.ora file includes parameters that configure Oracle Net features on Oracle database servers and clients. Using the parameters in the sqlnet.ora file, you can modify properties for connections in and out of the database.

For more information about why you might set sqlnet.ora parameters, see [Configuring profile parameters](#) in the Oracle documentation.

Setting sqlnet.ora parameters

Amazon RDS for Oracle parameter groups include a subset of sqlnet.ora parameters. You set them in the same way that you set other Oracle parameters. The `sqlnetora.` prefix identifies which parameters are sqlnet.ora parameters. For example, in an Oracle parameter group in Amazon RDS, the `default_sdu_size` sqlnet.ora parameter is `sqlnetora.default_sdu_size`.

For information about managing parameter groups and setting parameter values, see [Working with parameter groups \(p. 289\)](#).

Supported sqlnet.ora parameters

Amazon RDS supports the following sqlnet.ora parameters. Changes to dynamic sqlnet.ora parameters take effect immediately.

Parameter	Valid values	Static/ Dynamic	Description
<code>sqlnetora.default_sdu_size</code>	Oracle 12c – 512 to 2097152	Dynamic	The session data unit (SDU) size, in bytes. The SDU is the amount of data that is put in a buffer and sent across the network at one time.
<code>sqlnetora.diag_adr_enabled</code>	ON, OFF	Dynamic	A value that enables or disables Automatic Diagnostic Repository (ADR) tracing. ON specifies that ADR file tracing is used. OFF specifies that non-ADR file tracing is used.
<code>sqlnetora.recv_buf_size</code>	8192 to 268435456	Dynamic	The buffer space limit for receive operations of sessions, supported by the TCP/IP, TCP/IP with SSL, and SDP protocols.
<code>sqlnetora.send_buf_size</code>	8192 to 268435456	Dynamic	The buffer space limit for send operations of sessions, supported by the TCP/IP, TCP/IP with SSL, and SDP protocols.
<code>sqlnetora.sqlnet.allowed_logon_version_client</code>	8, 9, 10, 11, 12	Dynamic	Minimum authentication protocol version allowed for clients, and servers acting as clients, to establish a connection to Oracle DB instances.
<code>sqlnetora.sqlnet.allowed_logon_version_server</code>	8, 9, 10, 11, 12, 12a	Dynamic	Minimum authentication protocol version allowed to establish a connection to Oracle DB instances.
<code>sqlnetora.sqlnet.expire_time</code>	0 to 1440	Dynamic	Time interval, in minutes, to send a check to verify that client-server connections are active.

Parameter	Valid values	Static/ Dynamic	Description
sqlnetora.sqlnet.inbound_connect_timeout	0 or 10 to 7200	Dynamic	Time, in seconds, for a client to connect with the database server and provide the necessary authentication information.
sqlnetora.sqlnet.outbound_connect_timeout	0 or 10 to 7200	Dynamic	Time, in seconds, for a client to establish an Oracle Net connection to the DB instance.
sqlnetora.sqlnet.recv_timeout	0 or 10 to 7200	Dynamic	Time, in seconds, for a database server to wait for client data after establishing a connection.
sqlnetora.sqlnet.send_timeout	0 or 10 to 7200	Dynamic	Time, in seconds, for a database server to complete a send operation to clients after establishing a connection.
sqlnetora.tcp.connect_timeout	0 or 10 to 7200	Dynamic	Time, in seconds, for a client to establish a TCP connection to the database server.
sqlnetora.trace_level_server	0, 4, 10, 16, OFF, USER, ADMIN, SUPPORT	Dynamic	For non-ADR tracing, turns server tracing on at a specified level or turns it off.

The default value for each supported sqlnet.ora parameter is the Oracle default for the release. For information about default values for Oracle Database 12c, see [Parameters for the sqlnet.ora file](#) in the Oracle Database 12c documentation.

Viewing sqlnet.ora parameters

You can view sqlnet.ora parameters and their settings using the AWS Management Console, the AWS CLI, or a SQL client.

Viewing sqlnet.ora parameters using the console

For information about viewing parameters in a parameter group, see [Working with parameter groups \(p. 289\)](#).

In Oracle parameter groups, the `sqlnetora.` prefix identifies which parameters are sqlnet.ora parameters.

Viewing sqlnet.ora parameters using the AWS CLI

To view the sqlnet.ora parameters that were configured in an Oracle parameter group, use the AWS CLI `describe-db-parameters` command.

To view all of the sqlnet.ora parameters for an Oracle DB instance, call the AWS CLI `download-db-log-file-portion` command. Specify the DB instance identifier, the log file name, and the type of output.

Example

The following code lists all of the sqlnet.ora parameters for mydbinstance.

For Linux, macOS, or Unix:

```
aws rds download-db-log-file-portion \
--db-instance-identifier mydbinstance \
--log-file-name trace/sqlnet-parameters \
--output text
```

For Windows:

```
aws rds download-db-log-file-portion ^
--db-instance-identifier mydbinstance ^
--log-file-name trace/sqlnet-parameters ^
--output text
```

Viewing sqlnet.ora parameters using a SQL client

After you connect to the Oracle DB instance in a SQL client, the following query lists the sqlnet.ora parameters.

```
SELECT * FROM TABLE
(rdsadmin.rds_file_util.read_text_file(
    p_directory => 'BDUMP',
    p_filename  => 'sqlnet-parameters'));
```

For information about connecting to an Oracle DB instance in a SQL client, see [Connecting to your Oracle DB instance \(p. 1488\)](#).

Securing Oracle DB instance connections

Amazon RDS for Oracle supports SSL/TLS encrypted connections and also the Oracle Native Network Encryption (NNE) option to encrypt connections between your application and your Oracle DB instance. For more information about the Oracle Native Network Encryption option, see [Oracle native network encryption \(p. 1711\)](#).

Topics

- [Using SSL with an RDS for Oracle DB instance \(p. 1498\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1498\)](#)
- [Configuring Kerberos authentication for Amazon RDS for Oracle \(p. 1501\)](#)
- [Configuring UTL_HTTP access using certificates and an Oracle wallet \(p. 1513\)](#)

Using SSL with an RDS for Oracle DB instance

Secure Sockets Layer (SSL) is an industry-standard protocol for securing network connections between client and server. After SSL version 3.0, the name was changed to Transport Layer Security (TLS), but we still often refer to the protocol as SSL. Amazon RDS supports SSL encryption for Oracle DB instances. Using SSL, you can encrypt a connection between your application client and your Oracle DB instance. SSL support is available in all AWS Regions for Oracle.

To enable SSL encryption for an Oracle DB instance, add the Oracle SSL option to the option group associated with the DB instance. Amazon RDS uses a second port, as required by Oracle, for SSL connections. Doing this allows both clear text and SSL-encrypted communication to occur at the same time between a DB instance and an Oracle client. For example, you can use the port with clear text communication to communicate with other resources inside a VPC while using the port with SSL-encrypted communication to communicate with resources outside the VPC.

For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

Note

You can't use both SSL and Oracle native network encryption (NNE) on the same DB instance. Before you can use SSL encryption, you must disable any other connection encryption.

Updating applications to use new SSL/TLS certificates

As of September 19, 2019, Amazon RDS has published new Certificate Authority (CA) certificates for connecting to your RDS DB instances using Secure Socket Layer or Transport Layer Security (SSL/TLS). Following, you can find information about updating your applications to use the new certificates.

This topic can help you to determine whether any client applications use SSL/TLS to connect to your DB instances.

Important

When you change the certificate for an Amazon RDS for Oracle DB instance, only the database listener is restarted. The DB instance isn't restarted. Existing database connections are unaffected, but new connections will encounter errors for a brief period while the listener is restarted.

Note

For client applications that use SSL/TLS to connect to your DB instances, you must update your client application trust stores to include the new CA certificates.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB instances. We strongly recommend testing these procedures in a development or staging environment before implementing them in your production environments.

For more information about certificate rotation, see [Rotating your SSL/TLS certificate \(p. 2007\)](#). For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For information about using SSL/TLS with Oracle DB instances, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

Topics

- [Finding out whether applications connect using SSL \(p. 1499\)](#)
- [Updating your application trust store \(p. 1499\)](#)
- [Example Java code for establishing SSL connections \(p. 1500\)](#)

Finding out whether applications connect using SSL

If your Oracle DB instance uses an option group with the SSL option added, you might be using SSL. Check this by following the instructions in [Listing the options and option settings for an option group \(p. 281\)](#). For information about the SSL option, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

Check the listener log to determine whether there are SSL connections. The following is sample output in a listener log.

```
date time * (CONNECT_DATA=(CID=(PROGRAM=program)
(HOST=host)(USER=user))(SID=sid)) *
(ADDRESS=(PROTOCOL=tcp)(HOST=host)(PORT=port)) * establish * ORCL * 0
```

When PROTOCOL has the value tcps for an entry, it shows an SSL connection. However, when HOST is 127.0.0.1, you can ignore the entry. Connections from 127.0.0.1 are a local management agent on the DB instance. These connections aren't external SSL connections. Therefore, you have applications connecting using SSL if you see listener log entries where PROTOCOL is tcps and HOST is not 127.0.0.1.

To check the listener log, you can publish the log to Amazon CloudWatch Logs. For more information, see [Publishing Oracle logs to Amazon CloudWatch Logs \(p. 712\)](#).

Updating your application trust store

You can update the trust store for applications that use SQL*Plus or JDBC for SSL/TLS connections.

Updating your application trust store for SQL*Plus

You can update the trust store for applications that use SQL*Plus for SSL/TLS connections.

Note

When you update the trust store, you can retain older certificates in addition to adding the new certificates.

To update the trust store for SQL*Plus applications

1. Download the 2019 root certificate that works for all AWS Regions and put the file in the `ssl_wallet` directory.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

2. Run the following command to update the Oracle wallet.

```
prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert  
$ORACLE_HOME/ssl_wallet/rds-ca-2019-root.pem -auto_login_only
```

Replace the file name with the one that you downloaded.

3. Run the following command to confirm that the wallet was updated successfully.

```
prompt>orapki wallet display -wallet $ORACLE_HOME/ssl_wallet
```

Your output should contain the following.

```
Trusted Certificates:  
Subject: CN=Amazon RDS Root 2019 CA,OU=Amazon RDS,O=Amazon Web Services\  
Inc.,L=Seattle,ST=Washington,C=US
```

Updating your application trust store for JDBC

You can update the trust store for applications that use JDBC for SSL/TLS connections.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Example Java code for establishing SSL connections

The following code example shows how to set up the SSL connection using JDBC.

```
import java.sql.Connection;  
import java.sql.DriverManager;  
import java.sql.SQLException;  
import java.util.Properties;  
  
public class OracleSslConnectionTest {  
    private static final String DB_SERVER_NAME = "<dns-name-provided-by-amazon-rds>";  
    private static final Integer SSL_PORT = "<ssl-option-port-configured-in-option-group>";  
    private static final String DB_SID = "<oracle-sid>";  
    private static final String DB_USER = "<user name>";  
    private static final String DB_PASSWORD = "<password>";  
    // This key store has only the prod root ca.  
    private static final String KEY_STORE_FILE_PATH = "<file-path-to-keystore>";  
    private static final String KEY_STORE_PASS = "<keystore-password>";  
  
    public static void main(String[] args) throws SQLException {  
        final Properties properties = new Properties();  
        final String connectionString = String.format(  
            "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=%d))  
(CONNECT_DATA=(SID=%s)))",  
            DB_SERVER_NAME, SSL_PORT, DB_SID);  
        properties.put("user", DB_USER);  
        properties.put("password", DB_PASSWORD);  
        properties.put("oracle.jdbc.J2EE13Compliant", "true");  
        properties.put("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);  
        properties.put("javax.net.ssl.trustStoreType", "JKS");  
        properties.put("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);
```

```
        final Connection connection = DriverManager.getConnection(connectionString,
properties);
        // If no exception, that means handshake has passed, and an SSL connection can be
opened
    }
}
```

Important

After you have determined that your database connections use SSL/TLS and have updated your application trust store, you can update your database to use the rds-ca-2019 certificates. For instructions, see step 3 in [Updating your CA certificate by modifying your DB instance \(p. 2007\)](#).

Configuring Kerberos authentication for Amazon RDS for Oracle

You can use Kerberos authentication to authenticate users when they connect to your Amazon RDS for Oracle DB instance. In this configuration, your DB instance works with AWS Directory Service for Microsoft Active Directory, also called AWS Managed Microsoft AD. When users authenticate with an RDS for Oracle DB instance joined to the trusting domain, authentication requests are forwarded to the directory that you create with AWS Directory Service.

Keeping all of your credentials in the same directory can save you time and effort. You have a centralized place for storing and managing credentials for multiple database instances. A directory can also improve your overall security profile.

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of RDS for Oracle with Kerberos authentication, see [Kerberos authentication \(p. 101\)](#).

Note

Kerberos authentication isn't supported for DB instance classes that are deprecated for RDS for Oracle DB instances. For more information, see [RDS for Oracle instance classes \(p. 1477\)](#).

Topics

- [Setting up Kerberos authentication for Oracle DB instances \(p. 1501\)](#)
- [Managing a DB instance in a domain \(p. 1510\)](#)
- [Connecting to Oracle with Kerberos authentication \(p. 1512\)](#)

Setting up Kerberos authentication for Oracle DB instances

Use AWS Directory Service for Microsoft Active Directory, also called AWS Managed Microsoft AD, to set up Kerberos authentication for an Oracle DB instance. To set up Kerberos authentication, complete the following steps:

- [Step 1: Create a directory using the AWS Managed Microsoft AD \(p. 1502\)](#)
- [Step 2: Create a trust \(p. 1505\)](#)
- [Step 3: Configure IAM permissions for Amazon RDS \(p. 1505\)](#)
- [Step 4: Create and configure users \(p. 1507\)](#)
- [Step 5: Enable cross-VPC traffic between the directory and the DB instance \(p. 1507\)](#)
- [Step 6: Create or modify an Oracle DB instance \(p. 1507\)](#)
- [Step 7: Create Kerberos authentication Oracle logins \(p. 1509\)](#)

- [Step 8: Configure an Oracle client \(p. 1510\)](#)

Note

During the setup, RDS creates an Oracle database user named `managed_service_user@example.com` with the CREATE SESSION privilege, where `example.com` is your domain name. This user corresponds to the user that Directory Service creates inside your Managed Active Directory. Periodically, RDS uses the credentials provided by the Directory Service to log in to your Oracle database. Afterwards, RDS immediately destroys the ticket cache.

Step 1: Create a directory using the AWS Managed Microsoft AD

AWS Directory Service creates a fully managed Active Directory in the AWS Cloud. When you create an AWS Managed Microsoft AD directory, AWS Directory Service creates two domain controllers and Domain Name System (DNS) servers on your behalf. The directory servers are created in different subnets in a VPC. This redundancy helps make sure that your directory remains accessible even if a failure occurs.

When you create an AWS Managed Microsoft AD directory, AWS Directory Service performs the following tasks on your behalf:

- Sets up an Active Directory within the VPC.
- Creates a directory administrator account with the user name Admin and the specified password. You use this account to manage your directory.

Note

Be sure to save this password. AWS Directory Service doesn't store it. You can reset it, but you can't retrieve it.

- Creates a security group for the directory controllers.

When you launch an AWS Managed Microsoft AD, AWS creates an Organizational Unit (OU) that contains all of your directory's objects. This OU has the NetBIOS name that you typed when you created your directory and is located in the domain root. The domain root is owned and managed by AWS.

The Admin account that was created with your AWS Managed Microsoft AD directory has permissions for the most common administrative activities for your OU:

- Create, update, or delete users
- Add resources to your domain such as file or print servers, and then assign permissions for those resources to users in your OU
- Create additional OUs and containers
- Delegate authority
- Restore deleted objects from the Active Directory Recycle Bin
- Run AD and DNS Windows PowerShell modules on the Active Directory Web Service

The Admin account also has rights to perform the following domain-wide activities:

- Manage DNS configurations (add, remove, or update records, zones, and forwarders)
- View DNS event logs
- View security event logs

To create the directory, use the AWS Management Console, the AWS CLI, or the AWS Directory Service API. Make sure to open the relevant outbound ports on the directory security group so that the directory can communicate with the Oracle DB instance.

To create a directory with AWS Managed Microsoft AD

1. Sign in to the AWS Management Console and open the AWS Directory Service console at <https://console.aws.amazon.com/directoryservicev2/>.
2. In the navigation pane, choose **Directories** and choose **Set up Directory**.
3. Choose **AWS Managed Microsoft AD**. AWS Managed Microsoft AD is the only option that you can currently use with Amazon RDS.
4. Enter the following information:

Directory DNS name

The fully qualified name for the directory, such as **corp.example.com**.

Directory NetBIOS name

The short name for the directory, such as **CORP**.

Directory description

(Optional) A description for the directory.

Admin password

The password for the directory administrator. The directory creation process creates an administrator account with the user name Admin and this password.

The directory administrator password and can't include the word "admin." The password is case-sensitive and must be 8–64 characters in length. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a–z)
- Uppercase letters (A–Z)
- Numbers (0–9)
- Non-alphanumeric characters (~!@#\$%^&*_+=`|\{}{};:"<>,?./)

Confirm password

The administrator password retyped.

5. Choose **Next**.
6. Enter the following information in the **Networking** section and then choose **Next**:

VPC

The VPC for the directory. Create the Oracle DB instance in this same VPC.

Subnets

Subnets for the directory servers. The two subnets must be in different Availability Zones.

7. Review the directory information and make any necessary changes. When the information is correct, choose **Create directory**.

Review & create

Review

Directory type

Microsoft AD

VPC

vpc-8b6b78e9 ([REDACTED])

Directory DNS name

corp.example.com

Subnets

subnet-75128d10 ([REDACTED], us-east-1a)

subnet-f51665dd ([REDACTED], us-east-1b)

Directory NetBIOS name

CORP

Directory description

My directory

Pricing

Edition

Standard

Free trial eligible [Learn more](#)

30-day limited trial

~USD [REDACTED] *

* Includes two domain controllers, USD [REDACTED] /mo for each additional domain controller.

[Cancel](#)

[Previous](#)

[Create di...](#)

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to **Active**.

To see information about your directory, choose the directory name in the directory listing. Note the **Directory ID** value because you need this value when you create or modify your Oracle DB instance.

The screenshot shows the 'Directory details' page for a Microsoft AD directory. The 'Directory ID' field, which contains the value 'd-90670a8d36', is highlighted with a red oval. Other visible fields include 'Directory type' (Microsoft AD), 'Edition' (Standard), 'VPC' (vpc-6594f31c), 'Status' (Active), 'Subnets' (subnet-7d36a227, subnet-a2ab49c6), 'Last updated' (Tuesday, January 7, 2020), 'Availability zones' (us-east-1c, us-east-1d), 'Launch time' (Tuesday, January 7, 2020), 'DNS address' (redacted), and 'Description' (My directory). Below the table, there are tabs for 'Application management' (which is selected), 'Scale & share', 'Networking & security', and 'Maintenance'.

Step 2: Create a trust

If you plan to use AWS Managed Microsoft AD only, move on to [Step 3: Configure IAM permissions for Amazon RDS \(p. 1505\)](#).

To get Kerberos authentication using an on-premises or self-hosted Microsoft Active Directory, create a forest trust or external trust. The trust can be one-way or two-way. For more information about setting up forest trusts using AWS Directory Service, see [When to create a trust relationship](#) in the *AWS Directory Service Administration Guide*.

Step 3: Configure IAM permissions for Amazon RDS

To call AWS Directory Service for you, Amazon RDS requires an IAM role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`. This role allows Amazon RDS to make calls to the AWS Directory Service.

Note

For the role to allow access, the AWS Security Token Service (AWS STS) endpoint must be activated in the correct AWS Region for your AWS account. AWS STS endpoints are active by default in all AWS Regions, and you can use them without any further actions. For more information, see [Activating and deactivating AWS STS in an AWS Region](#) in the *IAM User Guide*.

Creating an IAM role

When you create a DB instance using the AWS Management Console, and the console user has the `iam:CreateRole` permission, the console creates `rds-directoryservice-kerberos-`

access-role automatically. Otherwise, you must create the IAM role manually. When you create an IAM role manually, choose Directory Service, and attach the AWS managed policy AmazonRDSDirectoryServiceAccess to it.

For more information about creating IAM roles for a service, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Note

The IAM role used for Windows Authentication for RDS for Microsoft SQL Server can't be used for RDS for Oracle.

Creating an IAM trust policy manually

Optionally, you can create resource policies with the required permissions instead of using the managed IAM policy AmazonRDSDirectoryServiceAccess. Specify both directoryservice.rds.amazonaws.com and rds.amazonaws.com as principals.

To limit the permissions that Amazon RDS gives another service for a specific resource, we recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies. The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of an Amazon RDS resource. For more information, see [Preventing cross-service confused deputy problems \(p. 2046\)](#).

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Amazon RDS to prevent the confused deputy problem.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "",  
            "Effect": "Allow",  
            "Principal": {  
                "Service": [  
                    "directoryservice.rds.amazonaws.com",  
                    "rds.amazonaws.com"  
                ]  
            },  
            "Action": "sts:AssumeRole",  
            "Condition": {  
                "ArnLike": {  
                    "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mydbinstance"  
                },  
                "StringEquals": {  
                    "aws:SourceAccount": "123456789012"  
                }  
            }  
        }  
    ]  
}
```

The role must also have the following IAM policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ds:DescribeDirectories",  
                "ds:AuthorizeApplication",  
                "ds:UnauthorizeApplication",  
                "ds:GetAuthorizedApplicationDetails"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Effect": "Allow",
        "Resource": "*"
    }
}
```

Step 4: Create and configure users

You can create users with the Active Directory Users and Computers tool, which is one of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. In this case, *users* are individual people or entities that have access to your directory.

To create users in an AWS Directory Service directory, you must be connected to a Windows-based Amazon EC2 instance that is a member of the AWS Directory Service directory. At the same time, you must be logged in as a user that has privileges to create users. For more information about creating users in your Microsoft Active Directory, see [Manage users and groups in AWS Managed Microsoft AD](#) in the [AWS Directory Service Administration Guide](#).

Step 5: Enable cross-VPC traffic between the directory and the DB instance

If you plan to locate the directory and the DB instance in the same VPC, skip this step and move on to [Step 6: Create or modify an Oracle DB instance \(p. 1507\)](#).

If you plan to locate the directory and the DB instance in different AWS accounts or VPCs, configure cross-VPC traffic using VPC peering or [AWS Transit Gateway](#). The following procedure enables traffic between VPCs using VPC peering. Follow the instructions in [What is VPC peering?](#) in the *Amazon Virtual Private Cloud Peering Guide*.

To enable cross-VPC traffic using VPC peering

1. Set up appropriate VPC routing rules to ensure that network traffic can flow both ways.
2. Ensure that the DB instance's security group can receive inbound traffic from the directory's security group. For more information, see [Best practices for AWS Managed Microsoft AD](#) in the [AWS Directory Service Administration Guide](#).
3. Ensure that there is no network access control list (ACL) rule to block traffic.

If a different AWS account owns the directory, you must share the directory.

To share the directory between AWS accounts

1. Start sharing the directory with the AWS account that the DB instance will be created in by following the instructions in [Tutorial: Sharing your AWS Managed Microsoft AD directory for seamless EC2 Domain-join](#) in the [AWS Directory Service Administration Guide](#).
2. Sign in to the AWS Directory Service console using the account for the DB instance, and ensure that the domain has the SHARED status before proceeding.
3. While signed into the AWS Directory Service console using the account for the DB instance, note the **Directory ID** value. You use this directory ID to join the DB instance to the domain.

Step 6: Create or modify an Oracle DB instance

Create or modify an Oracle DB instance for use with your directory. You can use the console, CLI, or RDS API to associate a DB instance with a directory. You can do this in one of the following ways:

- Create a new Oracle DB instance using the console, the [create-db-instance](#) CLI command, or the [CreateDBInstance](#) RDS API operation.

For instructions, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

- Modify an existing Oracle DB instance using the console, the [modify-db-instance](#) CLI command, or the [ModifyDBInstance](#) RDS API operation.

For instructions, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- Restore an Oracle DB instance from a DB snapshot using the console, the [restore-db-instance-from-db-snapshot](#) CLI command, or the [RestoreDBInstanceFromDBSnapshot](#) RDS API operation.

For instructions, see [Restoring from a DB snapshot \(p. 452\)](#).

- Restore an Oracle DB instance to a point-in-time using the console, the [restore-db-instance-to-point-in-time](#) CLI command, or the [RestoreDBInstanceToPointInTime](#) RDS API operation.

For instructions, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Kerberos authentication is only supported for Oracle DB instances in a VPC. The DB instance can be in the same VPC as the directory, or in a different VPC. When you create or modify the DB instance, do the following:

- Provide the domain identifier (d-* identifier) that was generated when you created your directory.
- Provide the name of the IAM role that you created.
- Ensure that the DB instance security group can receive inbound traffic from the directory security group and send outbound traffic to the directory.

When you use the console to create a DB instance, choose **Password and Kerberos authentication** in the **Database authentication** section. Choose **Browse Directory** and then select the directory, or choose **Create a new directory**.

Database authentication

Database authentication options [Info](#)

Password authentication
Authenticates using database passwords.

Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

Directory

Browse Directory

When you use the console to modify or restore a DB instance, choose the directory in the **Kerberos authentication** section, or choose **Create a new directory**.

Kerberos authentication

Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos authentication.

Directory

▼

[Create a new directory](#)

By choosing a directory and continuing with database instance creation you authorize Amazon RDS to create the IAM role necessary for using Kerberos authentication

When you use the AWS CLI, the following parameters are required for the DB instance to be able to use the directory that you created:

- For the `--domain` parameter, use the domain identifier ("d-*" identifier) generated when you created the directory.
- For the `--domain-iam-role-name` parameter, use the role you created that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

For example, the following CLI command modifies a DB instance to use a directory.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --domain d-ID \
  --domain-iam-role-name role-name
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --domain d-ID ^
  --domain-iam-role-name role-name
```

Important

If you modify a DB instance to enable Kerberos authentication, reboot the DB instance after making the change.

Note

`MANAGED_SERVICE_USER` is a service account whose name is randomly generated by Directory Service for RDS. During the Kerberos authentication setup, RDS for Oracle creates a user with the same name and assigns it the `CREATE SESSION` privilege. The Oracle DB user is identified externally as `MANAGED_SERVICE_USER@EXAMPLE.COM`, where `EXAMPLE.COM` is the name of your domain. Periodically, RDS uses the credentials provided by the Directory Service to log in to your Oracle database. Afterward, RDS immediately destroys the ticket cache.

Step 7: Create Kerberos authentication Oracle logins

Use the Amazon RDS master user credentials to connect to the Oracle DB instance as you do any other DB instance. The DB instance is joined to the AWS Managed Microsoft AD domain. Thus, you can provision Oracle logins and users from the Microsoft Active Directory users and groups in your domain. To manage database permissions, you grant and revoke standard Oracle permissions to these logins.

To allow a Microsoft Active Directory user to authenticate with Oracle

1. Connect to the Oracle DB instance using your Amazon RDS master user credentials.
2. Create an externally authenticated user in Oracle database.

In the following example, replace `KRBUSER@CORP.EXAMPLE.COM` with the user name and domain name.

```
CREATE USER "KRBUSER@CORP.EXAMPLE.COM" IDENTIFIED EXTERNALLY;
GRANT CREATE SESSION TO "KRBUSER@CORP.EXAMPLE.COM";
```

Users (both humans and applications) from your domain can now connect to the Oracle DB instance from a domain joined client machine using Kerberos authentication.

Step 8: Configure an Oracle client

To configure an Oracle client, meet the following requirements:

- Create a configuration file named krb5.conf (Linux) or krb5.ini (Windows) to point to the domain. Configure the Oracle client to use this configuration file.
- Verify that traffic can flow between the client host and AWS Directory Service over DNS port 53 over TCP/UDP, Kerberos ports (88 and 464 for managed AWS Directory Service) over TCP, and LDAP port 389 over TCP.
- Verify that traffic can flow between the client host and the DB instance over the database port.

Following is sample content for AWS Managed Microsoft AD.

```
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
    kdc = example.com
    admin_server = example.com
}
[domain_realm]
.example.com = CORP.EXAMPLE.COM
example.com = CORP.EXAMPLE.COM
```

Following is sample content for on-premise Microsoft AD. In your krb5.conf or krb5.ini file, replace *on-prem-ad-server-name* with the name of your on-premises AD server.

```
[libdefaults]
default_realm = ONPREM.COM
[realms]
AWSAD.COM = {
    kdc = awasad.com
    admin_server = awasad.com
}
ONPREM.COM = {
    kdc = on-prem-ad-server-name
    admin_server = on-prem-ad-server-name
}
[domain_realm]
.awasad.com = AWSAD.COM
awsad.com= AWSAD.COM
.onprem.com = ONPREM.COM
onprem.com= ONPREM.COM
```

Note

After you configure your krb5.ini or krb5.conf file, we recommend that you reboot the server.

The following is sample sqlnet.ora content for a SQL*Plus configuration:

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5PRE,KERBEROS5)
SQLNET.KERBEROS5_CONF=path_to_krb5.conf_file
```

For an example of a SQL Developer configuration, see [Document 1609359.1](#) from Oracle Support.

Managing a DB instance in a domain

You can use the console, the CLI, or the RDS API to manage your DB instance and its relationship with your Microsoft Active Directory. For example, you can associate a Microsoft Active Directory to enable Kerberos authentication. You can also disassociate a Microsoft Active Directory to disable Kerberos.

authentication. You can also move a DB instance to be externally authenticated by one Microsoft Active Directory to another.

For example, using the CLI, you can do the following:

- To reattempt enabling Kerberos authentication for a failed membership, use the [modify-db-instance](#) CLI command and specify the current membership's directory ID for the --domain option.
- To disable Kerberos authentication on a DB instance, use the [modify-db-instance](#) CLI command and specify none for the --domain option.
- To move a DB instance from one domain to another, use the [modify-db-instance](#) CLI command and specify the domain identifier of the new domain for the --domain option.

Viewing the status of domain membership

After you create or modify your DB instance, the DB instance becomes a member of the domain. You can view the status of the domain membership for the DB instance in the console or by running the [describe-db-instances](#) CLI command. The status of the DB instance can be one of the following:

- `kerberos-enabled` – The DB instance has Kerberos authentication enabled.
- `enabling-kerberos` – AWS is in the process of enabling Kerberos authentication on this DB instance.
- `pending-enable-kerberos` – Enabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-enable-kerberos` – AWS will attempt to enable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `pending-disable-kerberos` – Disabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-disable-kerberos` – AWS will attempt to disable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `enable-kerberos-failed` – A configuration problem has prevented AWS from enabling Kerberos authentication on the DB instance. Correct the configuration problem before reissuing the command to modify the DB instance.
- `disabling-kerberos` – AWS is in the process of disabling Kerberos authentication on this DB instance.

A request to enable Kerberos authentication can fail because of a network connectivity issue or an incorrect IAM role. If the attempt to enable Kerberos authentication fails when you create or modify a DB instance, make sure that you're using the correct IAM role. Then modify the DB instance to join the domain.

Note

Only Kerberos authentication with Amazon RDS for Oracle sends traffic to the domain's DNS servers. All other DNS requests are treated as outbound network access on your DB instances running Oracle. For more information about outbound network access with Amazon RDS for Oracle, see [Setting up a custom DNS server \(p. 1539\)](#).

Force-rotating Kerberos keys

A secret key is shared between AWS Managed Microsoft AD and Amazon RDS for Oracle DB instance. This key is rotated automatically every 45 days. You can use the following Amazon RDS procedure to force the rotation of this key.

```
SELECT rdsadmin.rdsadmin_kerberos_auth_tasks.rotate_kerberos_keytab AS TASK_ID FROM DUAL;
```

Note

In a read replica configuration, this procedure is available only on the source DB instance and not on the read replica.

The SELECT statement returns the ID of the task in a VARCHAR2 data type. You can view the status of an ongoing task in a bddump file. The bddump files are located in the /rdsdbdata/log/trace directory. Each bddump file name is in the following format.

```
dbtask-task-id.log
```

You can view the result by displaying the task's output file.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP', 'dbtask-task-id.log'));
```

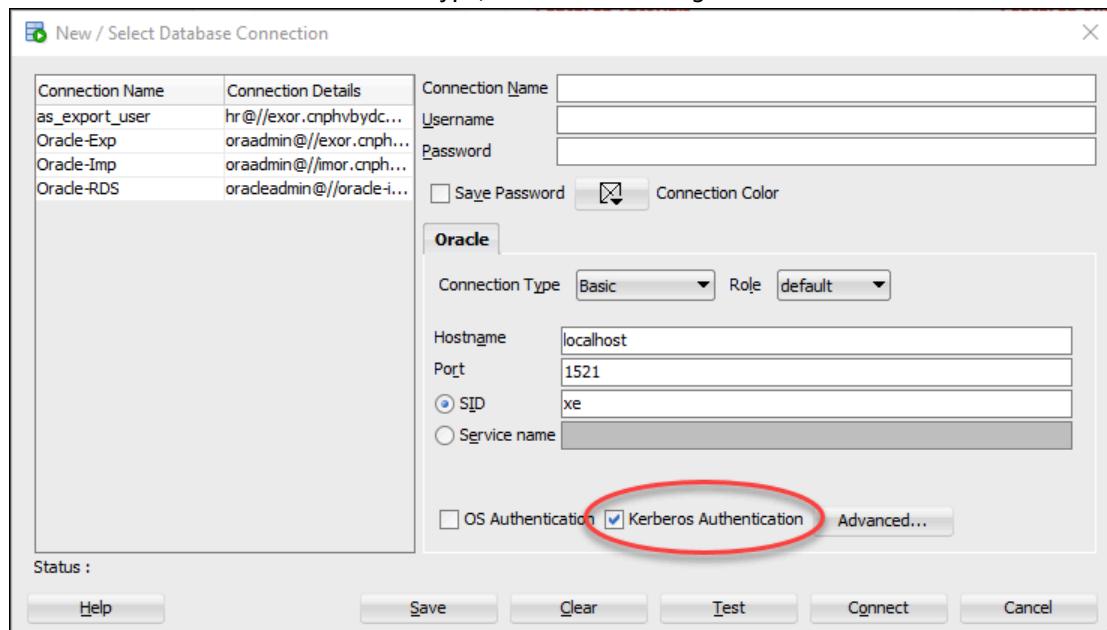
Replace *task-id* with the task ID returned by the procedure.

Note

Tasks are executed asynchronously.

Connecting to Oracle with Kerberos authentication

This section assumes that you have set up your Oracle client as described in [Step 8: Configure an Oracle client \(p. 1510\)](#). To connect to the Oracle DB with Kerberos authentication, log in using the Kerberos authentication type. For example, after launching Oracle SQL Developer, choose **Kerberos Authentication** as the authentication type, as shown following.



To connect to Oracle with Kerberos authentication with SQL*Plus:

1. At a command prompt, run the following command:

```
kinit username
```

Replace *username* with the user name and, at the prompt, enter the password stored in the Microsoft Active Directory for the user.

2. Open SQL*Plus and connect using the DNS name and port number for the Oracle DB instance.

For more information about connecting to an Oracle DB instance in SQL*Plus, see [Connecting to your DB instance using SQL*Plus \(p. 1492\)](#).

Configuring UTL_HTTP access using certificates and an Oracle wallet

Amazon RDS supports outbound network access on your Oracle DB instances. To connect your DB instance to the network, you can use the following PL/SQL packages:

UTL_HTTP

This package makes HTTP calls from SQL and PL/SQL. You can use it to access data on the Internet over HTTP. For more information, see [UTL_HTTP](#) in the Oracle documentation.

UTL_TCP

This package provides TCP/IP client-side access functionality in PL/SQL. This package is useful to PL/SQL applications that use Internet protocols and email. For more information, see [UTL_TCP](#) in the Oracle documentation.

UTL_SMTP

This package provides interfaces to the SMTP commands that enable a client to dispatch emails to an SMTP server. For more information, see [UTL_SMTP](#) in the Oracle documentation.

Before configuring your instance for network access, review the following requirements and considerations:

- To use SMTP with the UTL_MAIL option, see [Oracle UTL_MAIL \(p. 1753\)](#).
- The Domain Name Server (DNS) name of the remote host can be any of the following:
 - Publicly resolvable.
 - The endpoint of an Amazon RDS DB instance.
 - Resolvable through a custom DNS server. For more information, see [Setting up a custom DNS server \(p. 1539\)](#).
 - The private DNS name of an Amazon EC2 instance in the same VPC or a peered VPC. In this case, make sure that the name is resolvable through a custom DNS server. Alternatively, to use the DNS provided by Amazon, you can enable the enableDnsSupport attribute in the VPC settings and enable DNS resolution support for the VPC peering connection. For more information, see [DNS support in your VPC](#) and [Modifying your VPC peering connection](#).
- To connect securely to remote SSL/TLS resources, we recommend that you create and upload customized Oracle wallets. By using the Amazon S3 integration with Amazon RDS for Oracle feature, you can download a wallet from Amazon S3 into Oracle DB instances. For information about Amazon S3 integration for Oracle, see [Amazon S3 integration \(p. 1648\)](#).
- You can establish database links between Oracle DB instances over an SSL/TLS endpoint if the Oracle SSL option is configured for each instance. No further configuration is required. For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

By completing the following tasks, you can configure UTL_HTTP.REQUEST to work with websites that require client authentication certificates during the SSL handshake. You can also configure password authentication for UTL_HTTP access to websites by modifying the Oracle wallet generation commands and the DBMS_NETWORK_ACL_ADMIN.APPEND_WALLET_ACE procedure. For more information, see [DBMS_NETWORK_ACL_ADMIN](#) in the Oracle Database documentation.

Note

You can adapt the following tasks for UTL_SMTP, which enables you to send emails over SSL/TLS (including [Amazon Simple Email Service](#)).

Topics

- Step 1: Get the root certificate for a website (p. 1514)
- Step 2: Create an Oracle wallet (p. 1514)
- Step 3: Download your Oracle wallet to your RDS for Oracle instance (p. 1515)
- Step 4: Grant user permissions for the Oracle wallet (p. 1516)
- Step 5: Configure access to a website from your DB instance (p. 1517)
- Step 6: Test connections from your DB instance to a website (p. 1519)

Step 1: Get the root certificate for a website

For the RDS for Oracle instance to make secure connections to a website, add the root CA certificate. Amazon RDS uses the root certificate to sign the website certificate to the Oracle wallet.

You can get the root certificate in various ways. For example, you can do the following:

1. Use a web server to visit the website secured by the certificate.
2. Download the root certificate that was used for signing.

For AWS services, root certificates typically reside in the [Amazon trust services repository](#).

Step 2: Create an Oracle wallet

Create an Oracle wallet that contains both the web server certificates and the client authentication certificates. The RDS Oracle instance uses the web server certificate to establish a secure connection to the website. The website needs the client certificate to authenticate the Oracle database user.

You might want to configure secure connections without using client certificates for authentication. In this case, you can skip the Java keystore steps in the following procedure.

To create an Oracle wallet

1. Place the root and client certificates in a single directory, and then change into this directory.
2. Convert the .p12 client certificate to the Java keystore.

Note

If you're not using client certificates for authentication, you can skip this step.

The following example converts the client certificate named *client_certificate.p12* to the Java keystore named *client_keystore.jks*. The keystore is then included in the Oracle wallet. The keystore password is *P12PASSWORD*.

```
orapki wallet pkcs12_to_jks -wallet ./client_certificate.p12 -  
jksKeyStoreLoc ./client_keystore.jks -jksKeyStorepwd P12PASSWORD
```

3. Create a directory for your Oracle wallet that is different from the certificate directory.

The following example creates the directory /tmp/wallet.

```
mkdir -p /tmp/wallet
```

4. Create an Oracle wallet in your wallet directory.

The following example sets the Oracle wallet password to *P12PASSWORD*, which is the same password used by the Java keystore in a previous step. Using the same password is convenient, but not necessary. The *-auto_login* parameter turns on the automatic login feature, so that you don't need to specify a password every time you want to access it.

```
orapki wallet create -wallet /tmp/wallet -pwd P12PASSWORD -auto_login
```

5. Add the Java keystore to your Oracle wallet.

Note

If you're not using client certificates for authentication, you can skip this step.

The following example adds the keystore `client_keystore.jks` to the Oracle wallet named `/tmp/wallet`. In this example, you specify the same password for the Java keystore and the Oracle wallet.

```
orapki wallet jks_to_pkcs12 -wallet /tmp/wallet -pwd P12PASSWORD -  
keystore ./client_keystore.jks -jkspwd P12PASSWORD
```

6. Add the root certificate for your target website to the Oracle wallet.

The following example adds a certificate named `Root_CA.cer`.

```
orapki wallet add -wallet /tmp/wallet -trusted_cert -cert ./Root_CA.cer -  
pwd P12PASSWORD
```

7. Add any intermediate certificates.

The following example adds a certificate named `Intermediate.cer`. Repeat this step as many times as need to load all intermediate certificates.

```
orapki wallet add -wallet /tmp/wallet -trusted_cert -cert ./Intermediate.cer -  
pwd P12PASSWORD
```

8. Confirm that your newly created Oracle wallet has the required certificates.

```
orapki wallet display -wallet /tmp/wallet -pwd P12PASSWORD
```

Step 3: Download your Oracle wallet to your RDS for Oracle instance

In this step, you upload your Oracle wallet to Amazon S3, and then download the wallet from Amazon S3 to your RDS for Oracle instance.

To download your Oracle wallet to your RDS for Oracle DB instance

1. Complete the prerequisites for Amazon S3 integration with Oracle, and add the `S3_INTEGRATION` option to your Oracle DB instance. Ensure that the IAM role for the option has access to the Amazon S3 bucket you are using.

For more information, see [Amazon S3 integration \(p. 1648\)](#).

2. Log in to your DB instance as the master user, and then create an Oracle directory to hold the Oracle wallet.

The following example creates an Oracle directory named `WALLET_DIR`.

```
EXEC rdsadmin.rdsadmin_util.create_directory('WALLET_DIR');
```

For more information, see [Creating and dropping directories in the main data storage space \(p. 1597\)](#).

3. Upload the Oracle wallet to your Amazon S3 bucket.

You can use any supported upload technique.

4. If you're re-uploading an Oracle wallet, delete the existing wallet. Otherwise, skip to the next step.

The following example removes the existing wallet, which is named *cwallet.sso*.

```
EXEC UTL_FILE.FREMOVE ('WALLET_DIR','cwallet.sso');
```

5. Download the Oracle wallet from your Amazon S3 bucket to the Oracle DB instance.

The following example downloads the wallet named *cwallet.sso* from the Amazon S3 bucket named *my_s3_bucket* to the DB instance directory named *WALLET_DIR*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name    => 'my_s3_bucket',
    p_s3_prefix      => 'cwallet.sso',
    p_directory_name => 'WALLET_DIR')
AS TASK_ID FROM DUAL;
```

6. (Optional) Download a password-protected Oracle wallet.

Download this wallet only if you want to require a password for every use of the wallet. The following example downloads password-protected wallet *ewallet.p12*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name    => 'my_s3_bucket',
    p_s3_prefix      => 'ewallet.p12',
    p_directory_name => 'WALLET_DIR')
AS TASK_ID FROM DUAL;
```

7. Check the status of your DB task.

Substitute the task ID returned from the preceding steps for *dbtask-1234567890123-4567.log* in the following example.

```
SELECT TEXT FROM
TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1234567890123-4567.log'));
```

8. Check the contents of the directory that you're using to store the Oracle wallet.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'WALLET_DIR'));
```

For more information, see [Listing files in a DB instance directory \(p. 1598\)](#).

Step 4: Grant user permissions for the Oracle wallet

You can either create a new database user or configure an existing user. In either case, you must configure the user to access the Oracle wallet for secure connections and client authentication using certificates.

To grant user permissions for the Oracle wallet

1. Log in your RDS for Oracle DB instance as the master user.
2. If you don't want to configure an existing database user, create a new user. Otherwise, skip to the next step.

The following example creates a database user named *my-user*.

```
CREATE USER my-user IDENTIFIED BY my-user-pwd;
GRANT CONNECT TO my-user;
```

3. Grant permission to your database user on the directory containing your Oracle wallet.

The following example grants read access to user *my-user* on directory *WALLET_DIR*.

```
GRANT READ ON DIRECTORY WALLET_DIR TO my-user;
```

4. Grant permission to your database user to use the UTL_HTTP package.

The following PL/SQL program grants UTL_HTTP access to user *my-user*.

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('UTL_HTTP', UPPER('my-user'));
END;
/
```

5. Grant permission to your database user to use the UTL_FILE package.

The following PL/SQL program grants UTL_FILE access to user *my-user*.

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('UTL_FILE', UPPER('my-user'));
END;
/
```

Step 5: Configure access to a website from your DB instance

In this step, you configure your Oracle database user so that it can connect to your target website using UTL_HTTP, your uploaded Oracle Wallet, and the client certificate. For more information, see [Configuring Access Control to an Oracle Wallet](#) in the Oracle Database documentation.

To configure access to a website from your RDS for Oracle DB instance

1. Log in your RDS for Oracle DB instance as the master user.
2. Create a Host Access Control Entry (ACE) for your user and the target website on a secure port.

The following example configures *my-user* to access *secret.encrypted-website.com* on secure port 443.

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
    host      => 'secret.encrypted-website.com',
    lower_port => 443,
    upper_port => 443,
    ace       => xs$ace_type(privilege_list => xs$name_list('http'),
                           principal_name => 'my-user',
                           principal_type => xs_acl.ptype_db));
END;
/
```

For more information, see [Configuring Access Control for External Network Services](#) in the Oracle Database documentation.

3. (Optional) Create an ACE for your user and target website on the standard port.

You might need to use the standard port if some web pages are served from the standard web server port (80) instead of the secure port (443).

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
    host      => 'secret.encrypted-website.com',
    lower_port => 80,
    upper_port => 80,
    ace       => xs$ace_type(privilege_list => xs$name_list('http'),
                           principal_name => 'my-user',
                           principal_type => xs_acl.ptype_db));
END;
/
```

4. Confirm that the access control entries exist.

```
SET LINESIZE 150
COLUMN HOST FORMAT A40
COLUMN ACL FORMAT A50

SELECT HOST, LOWER_PORT, UPPER_PORT, ACL
  FROM DBA_NETWORK_ACLS
 ORDER BY HOST;
```

5. Grant permission to your database user to use the UTL_HTTP package.

The following PL/SQL program grants UTL_HTTP access to user *my-user*.

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('UTL_HTTP', UPPER('my-user'));
END;
/
```

6. Confirm that related access control lists exist.

```
SET LINESIZE 150
COLUMN ACL FORMAT A50
COLUMN PRINCIPAL FORMAT A20
COLUMN PRIVILEGE FORMAT A10

SELECT ACL, PRINCIPAL, PRIVILEGE, IS_GRANT,
       TO_CHAR(START_DATE, 'DD-MON-YYYY') AS START_DATE,
       TO_CHAR(END_DATE, 'DD-MON-YYYY') AS END_DATE
  FROM DBA_NETWORK_ACL_PRIVILEGES
 ORDER BY ACL, PRINCIPAL, PRIVILEGE;
```

7. Grant permission to your database user to use certificates for client authentication and your Oracle wallet for connections.

Note

If you're not using client certificates for authentication, you can skip this step.

```
DECLARE
  l_wallet_path all_directories.directory_path%type;
BEGIN
  SELECT DIRECTORY_PATH
    INTO l_wallet_path
    FROM ALL_DIRECTORIES
   WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';
  DBMS_NETWORK_ACL_ADMIN.APPEND_WALLET_ACE(
```

```

    wallet_path => 'file:' || l_wallet_path,
    ace          => xs$ace_type(privilege_list => xs
$name_list('use_client_certificates'),
                                principal_name => 'my-user',
                                principal_type => xs_acl.ptype_db));
END;
/

```

Step 6: Test connections from your DB instance to a website

In this step, you configure your database user so that it can connect to the website using UTL_HTTP, your uploaded Oracle Wallet, and the client certificate.

To configure access to a website from your RDS for Oracle DB instance

1. Log in your RDS for Oracle DB instance as a database user with UTL_HTTP permissions.
2. Confirm that a connection to your target website can resolve the host address.

The following example gets the host address from *secret.encrypted-website.com*.

```
SELECT UTL_INADDR.GET_HOST_ADDRESS(host => 'secret.encrypted-website.com')
  FROM DUAL;
```

3. Test a failed connection.

The following query fails because UTL_HTTP requires the location of the Oracle wallet with the certificates.

```
SELECT UTL_HTTP.REQUEST('secret.encrypted-website.com') FROM DUAL;
```

4. Test website access by using UTL_HTTP.SET_WALLET and selecting from DUAL.

```

DECLARE
  l_wallet_path all_directories.directory_path%type;
BEGIN
  SELECT DIRECTORY_PATH
    INTO l_wallet_path
    FROM ALL_DIRECTORIES
   WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';
  UTL_HTTP.SET_WALLET('file:' || l_wallet_path);
END;
/
SELECT UTL_HTTP.REQUEST('secret.encrypted-website.com') FROM DUAL;

```

5. (Optional) Test website access by storing your query in a variable and using EXECUTE IMMEDIATE.

```

DECLARE
  l_wallet_path all_directories.directory_path%type;
  v_webpage_sql VARCHAR2(1000);
  v_results      VARCHAR2(32767);
BEGIN
  SELECT DIRECTORY_PATH
    INTO l_wallet_path
    FROM ALL_DIRECTORIES
   WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';

```

```
v_webpage_sql := 'SELECT UTL_HTTP.REQUEST('''secret.encrypted-website.com''', ''',  
'file:' || l_wallet_path||'''') FROM DUAL';  
DBMS_OUTPUT.PUT_LINE(v_webpage_sql);  
EXECUTE IMMEDIATE v_webpage_sql INTO v_results;  
DBMS_OUTPUT.PUT_LINE(v_results);  
END;  
/
```

6. (Optional) Find the file system location of your Oracle wallet directory.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'WALLET_DIR'));
```

Use the output from the previous command to make an HTTP request. For example, if the directory is *rdsdbdata/userdirs/01*, run the following query.

```
SELECT UTL_HTTP.REQUEST('https://secret.encrypted-website.com/', '', 'file://rdsdbdata/  
userdirs/01')  
FROM DUAL;
```

Administering your Oracle DB instance

Following are the common management tasks that you perform with an Amazon RDS DB instance. Some tasks are the same for all RDS DB instances. Other tasks are specific to RDS for Oracle.

The following tasks are common to all RDS databases, but Oracle has special considerations. For example, connect to an Oracle Database using the Oracle clients SQL*Plus and SQL Developer.

Task area	Relevant documentation
Instance classes, storage, and PIOPS If you are creating a production instance, learn how instance classes, storage types, and Provisioned IOPS work in Amazon RDS.	RDS for Oracle instance classes (p. 1477) Amazon RDS storage types (p. 64)
Multi-AZ deployments A production DB instance should use Multi-AZ deployments. Multi-AZ deployments provide increased availability, data durability, and fault tolerance for DB instances.	Multi-AZ deployments for high availability (p. 121)
Amazon VPC If your AWS account has a default virtual private cloud (VPC), then your DB instance is automatically created inside the default VPC. If your account doesn't have a default VPC, and you want the DB instance in a VPC, create the VPC and subnet groups before you create the instance.	Working with a DB instance in a VPC (p. 2103)
Security groups By default, DB instances use a firewall that prevents access. Make sure that you create a security group with the correct IP addresses and network configuration to access the DB instance.	Controlling access with security groups (p. 2085)
Parameter groups If your DB instance is going to require specific database parameters, create a parameter group before you create the DB instance.	Working with parameter groups (p. 289)
Option groups If your DB instance requires specific database options, create an option group before you create the DB instance.	Adding options to Oracle DB instances (p. 1646)
Connecting to your DB instance After creating a security group and associating it to a DB instance, you can connect to the DB instance using any standard SQL client application such as Oracle SQL*Plus.	Connecting to your Oracle DB instance (p. 1488)
Backup and restore You can configure your DB instance to take automated backups, or take manual snapshots, and then restore instances from the backups or snapshots.	Backing up and restoring an Amazon RDS DB instance (p. 426)

Task area	Relevant documentation
Monitoring You can monitor an Oracle DB instance by using CloudWatch Amazon RDS metrics, events, and enhanced monitoring.	Viewing metrics in the Amazon RDS console (p. 525) Viewing Amazon RDS events (p. 647)
Log files You can access the log files for your Oracle DB instance.	Monitoring Amazon RDS log files (p. 680)

Following, you can find a description for Amazon RDS–specific implementations of common DBA tasks for RDS Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. Also, RDS restricts access to certain system procedures and tables that require advanced privileges. In many of the tasks, you run the `rdsadmin` package, which is an Amazon RDS–specific tool that enables you to administer your database.

The following are common DBA tasks for DB instances running Oracle:

- [System tasks \(p. 1529\)](#)

Disconnecting a session (p. 1529)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.disconnect</code> Oracle method: <code>alter system disconnect session</code>
Terminating a session (p. 1530)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.kill</code> Oracle method: <code>alter system kill session</code>
Canceling a SQL statement in a session (p. 1531)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.cancel</code> Oracle method: <code>alter system cancel sql</code>
Enabling and disabling restricted sessions (p. 1532)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.restricted_session</code> Oracle method: <code>alter system enable restricted session</code>
Flushing the shared pool (p. 1532)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.flush_shared_pool</code> Oracle method: <code>alter system flush shared_pool</code>
Flushing the buffer cache (p. 1533)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.flush_buffer_cache</code> Oracle method: <code>alter system flush buffer_cache</code>
Granting SELECT or EXECUTE privileges to SYS objects (p. 1533)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.grant_sys_object</code> Oracle method: <code>grant</code>
Revoking SELECT or EXECUTE privileges on SYS objects (p. 1534)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.revoke_sys_object</code> Oracle method: <code>revoke</code>

Granting privileges to non-master users (p. 1535)	Amazon RDS method: <code>grant</code> Oracle method: <code>grant</code>
Creating custom functions to verify passwords (p. 1536)	Amazon RDS method: <code>rdsadmin.rdsadmin_password_verify.create_verify_function</code> Amazon RDS method: <code>rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn</code>
Setting up a custom DNS server (p. 1539)	—
Listing allowed system diagnostic events (p. 1540)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.list_allowed_system_events</code> Oracle method: —
Setting system diagnostic events (p. 1541)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.set_allowed_system_events</code> Oracle method: <code>ALTER SYSTEM SET EVENTS '<i>set_event_clause</i>'</code>
Listing system diagnostic events that are set (p. 1542)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.list_set_system_events</code> Oracle method: <code>ALTER SESSION SET EVENTS 'IMMEDIATE EVENTDUMP(SYSTEM)'</code>
Unsetting system diagnostic events (p. 1542)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.unset_system_event</code> Oracle method: <code>ALTER SYSTEM SET EVENTS '<i>unset_event_clause</i>'</code>

- [Database tasks \(p. 1543\)](#)

Changing the global name of a database (p. 1543)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.rename_global_name</code> Oracle method: <code>alter database rename</code>
Creating and sizing tablespaces (p. 1544)	Amazon RDS method: <code>create tablespace</code> Oracle method: <code>alter database</code>
Setting the default tablespace (p. 1544)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.alter_default_tablespace</code> Oracle method: <code>alter database default tablespace</code>
Setting the default temporary tablespace (p. 1545)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.alter_default_temp_tablespace</code> Oracle method: <code>alter database default temporary tablespace</code>

Creating a temporary tablespace on the instance store (p. 1545)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace</code> Oracle method: <code>create temporary tablespace</code>
Checkpointing a database (p. 1547)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.checkpoint</code> Oracle method: <code>alter system checkpoint</code>
Setting distributed recovery (p. 1547)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.enable_distr_recovery</code> Oracle method: <code>alter system enable distributed recovery</code>
Setting the database time zone (p. 1547)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.alter_db_time_zone</code> Oracle method: <code>alter database set time_zone</code>
Working with Oracle external tables (p. 1548)	—
Generating performance reports with Automatic Workload Repository (AWR) (p. 1549)	Amazon RDS method: <code>rdsadmin.rdsadmin_diagnostic_util.procedures</code> Oracle method: <code>dbms_workload_repository package</code>
Adjusting database links for use with DB instances in a VPC (p. 1553)	—
Setting the default edition for a DB instance (p. 1553)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.alter_default_edition</code> Oracle method: <code>alter database default edition</code>
Enabling auditing for the SYS.AUD\$ table (p. 1553)	Amazon RDS method: <code>rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table</code> Oracle method: <code>audit</code>
Disabling auditing for the SYS.AUD\$ table (p. 1554)	Amazon RDS method: <code>rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table</code> Oracle method: <code>noaudit</code>
Cleaning up interrupted online index builds (p. 1554)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_repair.online_index_clean</code> Oracle method: <code>dbms_repair.online_index_clean</code>
Skipping corrupt blocks (p. 1555)	Amazon RDS method: Several <code>rdsadmin.rdsadmin_dbms_repair</code> procedures Oracle method: <code>dbms_repair package</code>

Resizing the temporary tablespace in a read replica (p. 1557)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.resize_temp_tablespace</code> or <code>rdsadmin.rdsadmin_util.resize_tempfile</code> procedure Oracle method: —
Purging the recycle bin (p. 1558)	Amazon RDS method: EXEC <code>rdsadmin.rdsadmin_util.purge_dba_recyclebin</code> Oracle method: <code>purge dba_recyclebin</code>
Setting the Data Redaction policy for full redaction (p. 1558)	Amazon RDS method: EXEC <code>rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val</code> Oracle method: exec <code>dbms_redact.UPDATE_FULL_REDACTION_VALUES</code>

- [Log tasks \(p. 1560\)](#)

Setting force logging (p. 1560)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.force_logging</code> Oracle method: <code>alter database force logging</code>
Setting supplemental logging (p. 1561)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.alter_suppl</code> Oracle method: <code>alter database add supplemental log</code>
Switching online log files (p. 1561)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.switch_logfi</code> Oracle method: <code>alter system switch logfile</code>
Adding online redo logs (p. 1562)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.add_logfile</code>
Dropping online redo logs (p. 1562)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.drop_logfile</code>
Resizing online redo logs (p. 1563)	—
Retaining archived redo logs (p. 1564)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.set_configur</code>
Downloading archived redo logs from Amazon S3 (p. 1566)	Amazon RDS method: <code>rdsadmin.rdsadmin_archive_log_downl</code> Amazon RDS method: <code>rdsadmin.rdsadmin_archive_log_downl</code>

[Accessing online and archived redo logs \(p. 1566\)](#)

Amazon RDS method:
`rdsadmin.rdsadmin_master_util.create`

Amazon RDS method:
`rdsadmin.rdsadmin_master_util.create`

- [RMAN tasks \(p. 1568\)](#)

[Validating DB instance files \(p. 1571\)](#)

Amazon RDS method:
`rdsadmin_rman_util.procedure`

Oracle method: RMAN
VALIDATE

[Enabling and disabling block change tracking \(p. 1574\)](#)

Amazon RDS method:
`rdsadmin_rman_util.procedure`

Oracle method: ALTER
DATABASE

[Crosschecking archived redo logs \(p. 1575\)](#)

Amazon RDS method:
`rdsadmin_rman_util.crosscheck_archi`

Oracle method: RMAN BACKUP

[Backing up archived redo logs \(p. 1576\)](#)

Amazon RDS method:
`rdsadmin_rman_util.procedure`

Oracle method: RMAN BACKUP

[Performing a full database backup \(p. 1581\)](#)

Amazon RDS method:
`rdsadmin_rman_util.backup_database`

Oracle method: RMAN BACKUP

[Performing an incremental database backup \(p. 1582\)](#)

Amazon RDS method:
`rdsadmin_rman_util.backup_database`

Oracle method: RMAN BACKUP

[Backing up a tablespace \(p. 1583\)](#)

Amazon RDS method:
`rdsadmin_rman_util.backup_database`

Oracle method: RMAN BACKUP

- [Oracle Scheduler tasks \(p. 1585\)](#)

[Modifying DBMS_SCHEDULER jobs \(p. 1586\)](#)

Amazon RDS method:
`dbms_scheduler.set_attribute`

Oracle method:
`dbms_scheduler.set_attribute`

Modifying AutoTask maintenance windows (p. 1586)	Amazon RDS method: <code>dbms_scheduler.set_attribute</code> Oracle method: <code>dbms_scheduler.set_attribute</code>
Setting the time zone for Oracle Scheduler jobs (p. 1587)	Amazon RDS method: <code>dbms_scheduler.set_scheduler_attribute</code> Oracle method: <code>dbms_scheduler.set_scheduler_attribute</code>
Turning off Oracle Scheduler jobs owned by SYS (p. 1588)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_scheduler.disable</code> Oracle method: <code>dbms_scheduler.disable</code>
Turning on Oracle Scheduler jobs owned by SYS (p. 1588)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_scheduler.enable</code> Oracle method: <code>dbms_scheduler.enable</code>
Modifying the Oracle Scheduler repeat interval for jobs of CALENDAR type (p. 1589)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_scheduler.set_attribute</code> Oracle method: <code>dbms_scheduler.set_attribute</code>
Modifying the Oracle Scheduler repeat interval for jobs of NAMED type (p. 1589)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_scheduler.set_attribute</code> Oracle method: <code>dbms_scheduler.set_attribute</code>
Turning off autocommit for Oracle Scheduler job creation (p. 1590)	Amazon RDS method: <code>rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag</code> Oracle method: <code>dbms_isched.set_no_commit_flag</code>

- [Diagnostic tasks \(p. 1590\)](#)

Listing incidents (p. 1591)	Amazon RDS method: <code>rdsadmin.rdsadmin_adrci_util.list_incident</code> Oracle method: ADRCI command <code>show incident</code>
Listing problems (p. 1593)	Amazon RDS method: <code>rdsadmin.rdsadmin_adrci_util.list_problem</code> Oracle method: ADRCI command <code>show problem</code>

Creating incident packages (p. 1594)	Amazon RDS method: <code>rdsadmin.rdsadmin_adrci_util.create</code> Oracle method: ADRCI command <code>ips create package</code>
Showing trace files (p. 1595)	Amazon RDS method: <code>rdsadmin.rdsadmin_adrci_util.show_a</code> Oracle method: ADRCI command <code>show tracefile</code>

- [Other tasks \(p. 1597\)](#)

Creating and dropping directories in the main data storage space (p. 1597)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.create_directory</code> Oracle method: <code>CREATE DIRECTORY</code> Amazon RDS method: <code>rdsadmin.rdsadmin_util.drop_directory</code> Oracle method: <code>DROP DIRECTORY</code>
Listing files in a DB instance directory (p. 1598)	Amazon RDS method: <code>rdsadmin.rds_file_util.listdir</code> Oracle method: —
Reading files in a DB instance directory (p. 1598)	Amazon RDS method: <code>rdsadmin.rds_file_util.read_text_file</code> Oracle method: —
Accessing Opatch files (p. 1599)	Amazon RDS method: <code>rdsadmin.rds_file_util.read_text_file</code> or <code>rdsadmin.tracefile_listing</code> Oracle method: <code>opatch</code>
Setting parameters for advisor tasks (p. 1601)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.advisor_task</code> Oracle method: Various stored package procedures
Disabling AUTO_STATS_ADVISOR_TASK (p. 1602)	Amazon RDS method: <code>rdsadmin.rdsadmin_util.advisor_task</code> Oracle method: —

[Re-enabling AUTO_STATS_ADVISOR_TASK \(p. 1603\)](#)

Amazon RDS method:

`rdsadmin.rdsadmin_util.dbms_stats_i`

Oracle method: —

You can also use Amazon RDS procedures for Amazon S3 integration with Oracle and for running OEM Management Agent database tasks. For more information, see [Amazon S3 integration \(p. 1648\)](#) and [Performing database tasks with the Management Agent \(p. 1699\)](#).

Performing common system tasks for Oracle DB instances

Following, you can find how to perform certain common DBA tasks related to the system on your Amazon RDS DB instances running Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances, and restricts access to certain system procedures and tables that require advanced privileges.

Topics

- [Disconnecting a session \(p. 1529\)](#)
- [Terminating a session \(p. 1530\)](#)
- [Canceling a SQL statement in a session \(p. 1531\)](#)
- [Enabling and disabling restricted sessions \(p. 1532\)](#)
- [Flushing the shared pool \(p. 1532\)](#)
- [Flushing the buffer cache \(p. 1533\)](#)
- [Flushing the database smart flash cache \(p. 1533\)](#)
- [Granting SELECT or EXECUTE privileges to SYS objects \(p. 1533\)](#)
- [Revoking SELECT or EXECUTE privileges on SYS objects \(p. 1534\)](#)
- [Granting privileges to non-master users \(p. 1535\)](#)
- [Creating custom functions to verify passwords \(p. 1536\)](#)
- [Setting up a custom DNS server \(p. 1539\)](#)
- [Setting and unsetting system diagnostic events \(p. 1540\)](#)

Disconnecting a session

To disconnect the current session by ending the dedicated server process, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.disconnect`. The `disconnect` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>sid</code>	number	—	Yes	The session identifier.
<code>serial</code>	number	—	Yes	The serial number of the session.
<code>method</code>	varchar	'IMMEDIATE'	No	Valid values are 'IMMEDIATE' or 'POST_TRANSACTION'.

The following example disconnects a session.

```
begin
    rdsadmin.rdsadmin_util.disconnect(
        sid    => sid,
        serial => serial_number);
end;
/
```

To get the session identifier and the session serial number, query the V\$SESSION view. The following example gets all sessions for the user *AWSUSER*.

```
SELECT SID, SERIAL#, STATUS FROM V$SESSION WHERE USERNAME = 'AWSUSER';
```

The database must be open to use this method. For more information about disconnecting a session, see [ALTER SYSTEM](#) in the Oracle documentation.

Terminating a session

To terminate a session, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.kill`. The `kill` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>sid</code>	number	—	Yes	The session identifier.
<code>serial</code>	number	—	Yes	The serial number of the session.
<code>method</code>	varchar	null	No	<p>Valid values are 'IMMEDIATE' or 'PROCESS'. If you specify IMMEDIATE, it has the same effect as running the following statement:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>ALTER SYSTEM KILL SESSION 'sid,serial#' IMMEDIATE</pre> </div> <p>If you specify PROCESS, you terminate the processes associated with a session. Only specify PROCESS if terminating the session using IMMEDIATE was unsuccessful.</p>

To get the session identifier and the session serial number, query the V\$SESSION view. The following example gets all sessions for the user *AWSUSER*.

```
SELECT SID, SERIAL#, STATUS FROM V$SESSION WHERE USERNAME = 'AWSUSER';
```

The following example terminates a session.

```

BEGIN
    rdsadmin.rdsadmin_util.kill(
        sid    => sid,
        serial => serial_number,
        method => 'IMMEDIATE');
END;
/

```

The following example terminates the processes associated with a session.

```

BEGIN
    rdsadmin.rdsadmin_util.kill(
        sid    => sid,
        serial => serial_number,
        method => 'PROCESS');
END;
/

```

Cancelling a SQL statement in a session

To cancel a SQL statement in a session, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.cancel`.

Note

This procedure is supported for Oracle Database 19c (19.0.0) and all higher major and minor versions of RDS for Oracle.

The `cancel` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>sid</code>	number	—	Yes	The session identifier.
<code>serial</code>	number	—	Yes	The serial number of the session.
<code>sql_id</code>	varchar2	null	No	The SQL identifier of the SQL statement.

The following example cancels a SQL statement in a session.

```

begin
    rdsadmin.rdsadmin_util.cancel(
        sid    => sid,
        serial => serial_number,
        sql_id => sql_id);
end;
/

```

To get the session identifier, the session serial number, and the SQL identifier of a SQL statement, query the `V$SESSION` view. The following example gets all sessions and SQL identifiers for the user `AWSUSER`.

```
select SID, SERIAL#, SQL_ID, STATUS from V$SESSION where USERNAME = 'AWSUSER';
```

Enabling and disabling restricted sessions

To enable and disable restricted sessions, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.restricted_session`. The `restricted_session` procedure has the following parameters.

Parameter name	Data type	Default	Yes	Description
<code>p_enable</code>	boolean	true	No	Set to true to enable restricted sessions, false to disable restricted sessions.

The following example shows how to enable and disable restricted sessions.

```
/* Verify that the database is currently unrestricted. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
-----
ALLOWED

/* Enable restricted sessions */

EXEC rdsadmin.rdsadmin_util.restricted_session(p_enable => true);

/* Verify that the database is now restricted. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
-----
RESTRICTED

/* Disable restricted sessions */

EXEC rdsadmin.rdsadmin_util.restricted_session(p_enable => false);

/* Verify that the database is now unrestricted again. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
-----
ALLOWED
```

Flushing the shared pool

To flush the shared pool, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.flush_shared_pool`. The `flush_shared_pool` procedure has no parameters.

The following example flushes the shared pool.

```
EXEC rdsadmin.rdsadmin_util.flush_shared_pool;
```

Flushing the buffer cache

To flush the buffer cache, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.flush_buffer_cache`. The `flush_buffer_cache` procedure has no parameters.

The following example flushes the buffer cache.

```
EXEC rdsadmin.rdsadmin_util.flush_buffer_cache;
```

Flushing the database smart flash cache

To flush the database smart flash cache, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.flush_flash_cache`. The `flush_flash_cache` procedure has no parameters. The following example flushes the database smart flash cache.

```
EXEC rdsadmin.rdsadmin_util.flush_flash_cache;
```

For more information about using the database smart flash cache with RDS for Oracle, see [Storing temporary data in an RDS for Oracle instance store \(p. 1604\)](#).

Granting SELECT or EXECUTE privileges to SYS objects

Usually you transfer privileges by using roles, which can contain many objects. To grant privileges to a single object, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.grant_sys_object`. The procedure grants only privileges that the master user has already been granted through a role or direct grant.

The `grant_sys_object` procedure has the following parameters.

Important

For all parameter values, use uppercase unless you created the user with a case-sensitive identifier. For example, if you run `CREATE USER myuser` or `CREATE USER MYUSER`, the data dictionary stores `MYUSER`. However, if you use double quotes in `CREATE USER "MyUser"`, the data dictionary stores `MyUser`.

Parameter name	Data type	Default	Required	Description
<code>p_obj_name</code>	<code>varchar2</code>	—	Yes	The name of the object to grant privileges for. The object can be a directory, function, package, procedure, sequence, table, or view. Object names must be spelled exactly as they appear in <code>DBA_OBJECTS</code> . Most system objects are defined in uppercase, so we recommend that you try that first.
<code>p_grantee</code>	<code>varchar2</code>	—	Yes	The name of the object to grant privileges to. The object can be a schema or a role.

Parameter name	Data type	Default	Required	Description
p_privilege	varchar2	null	Yes	—
p_grant_option	boolean	false	No	Set to true to use the with grant option. The p_grant_option parameter is supported for 12.1.0.2.v4 and later, all 12.2.0.1 versions, and all 19.0.0 versions.

The following example grants select privileges on an object named V_\$SESSION to a user named USER1.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_grantee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

The following example grants select privileges on an object named V_\$SESSION to a user named USER1 with the grant option.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_grantee   => 'USER1',
        p_privilege => 'SELECT',
        p_grant_option => true);
end;
/
```

To be able to grant privileges on an object, your account must have those privileges granted to it directly with the grant option, or via a role granted using with admin option. In the most common case, you may want to grant SELECT on a DBA view that has been granted to the SELECT_CATALOG_ROLE role. If that role isn't already directly granted to your user using with admin option, then you can't transfer the privilege. If you have the DBA privilege, then you can grant the role directly to another user.

The following example grants the SELECT_CATALOG_ROLE and EXECUTE_CATALOG_ROLE to USER1. Since the with admin option is used, USER1 can now grant access to SYS objects that have been granted to SELECT_CATALOG_ROLE.

```
GRANT SELECT_CATALOG_ROLE TO USER1 WITH ADMIN OPTION;
GRANT EXECUTE_CATALOG_ROLE to USER1 WITH ADMIN OPTION;
```

Objects already granted to PUBLIC do not need to be re-granted. If you use the grant_sys_object procedure to re-grant access, the procedure call succeeds.

Revoking SELECT or EXECUTE privileges on SYS objects

To revoke privileges on a single object, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.revoke_sys_object`. The procedure only revokes privileges that the master account has already been granted through a role or direct grant.

The `revoke_sys_object` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_obj_name	varchar2	—	Yes	The name of the object to revoke privileges for. The object can be a directory, function, package, procedure, sequence, table, or view. Object names must be spelled exactly as they appear in DBA_OBJECTS. Most system objects are defined in upper case, so we recommend you try that first.
p_revokee	varchar2	—	Yes	The name of the object to revoke privileges for. The object can be a schema or a role.
p_privilege	varchar2	null	Yes	—

The following example revokes select privileges on an object named V_\$SESSION from a user named USER1.

```
begin
    rdsadmin.rdsadmin_util.revoke_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_revokee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

Granting privileges to non-master users

You can grant select privileges for many objects in the SYS schema by using the SELECT_CATALOG_ROLE role. The SELECT_CATALOG_ROLE role gives users SELECT privileges on data dictionary views. The following example grants the role SELECT_CATALOG_ROLE to a user named *user1*.

```
GRANT SELECT_CATALOG_ROLE TO user1;
```

You can grant EXECUTE privileges for many objects in the SYS schema by using the EXECUTE_CATALOG_ROLE role. The EXECUTE_CATALOG_ROLE role gives users EXECUTE privileges for packages and procedures in the data dictionary. The following example grants the role EXECUTE_CATALOG_ROLE to a user named *user1*.

```
GRANT EXECUTE_CATALOG_ROLE TO user1;
```

The following example gets the permissions that the roles SELECT_CATALOG_ROLE and EXECUTE_CATALOG_ROLE allow.

```
SELECT *
  FROM ROLE_TAB_PRIVS
```

```
WHERE ROLE IN ('SELECT_CATALOG_ROLE', 'EXECUTE_CATALOG_ROLE')
ORDER BY ROLE, TABLE_NAME ASC;
```

The following example creates a non-master user named `user1`, grants the `CREATE SESSION` privilege, and grants the `SELECT` privilege on a database named `sh.sales`.

```
CREATE USER user1 IDENTIFIED BY PASSWORD;
GRANT CREATE SESSION TO user1;
GRANT SELECT ON sh.sales TO user1;
```

Creating custom functions to verify passwords

You can create a custom password verification function in the following ways:

- To use standard verification logic, and to store your function in the `SYS` schema, use the `create_verify_function` procedure.
- To use custom verification logic, or to avoid storing your function in the `SYS` schema, use the `create_passthrough_verify_fcn` procedure.

The `create_verify_function` procedure

You can create a custom function to verify passwords by using the Amazon RDS procedure `rdsadmin.rdsadmin_password_verify.create_verify_function`. The `create_verify_function` procedure is supported for version 12.1.0.2.v5 and all higher major and minor versions of RDS for Oracle.

The `create_verify_function` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_verify_function_name</code>	varchar2	—	Yes	The name for your custom function. This function is created for you in the <code>SYS</code> schema. You assign this function to user profiles.
<code>p_min_length</code>	number	8	No	The minimum number of characters required.
<code>p_max_length</code>	number	256	No	The maximum number of characters allowed.
<code>p_min_letters</code>	number	1	No	The minimum number of letters required.
<code>p_min_uppercase</code>	number	0	No	The minimum number of uppercase letters required.
<code>p_min_lowercase</code>	number	0	No	The minimum number of lowercase letters required.
<code>p_min_digits</code>	number	1	No	The minimum number of digits required.
<code>p_min_special</code>	number	0	No	The minimum number of special characters required.

Parameter name	Data type	Default	Required	Description
p_min_different_chars	number	3	No	The minimum number of different characters required between the old and new password.
p_disallow_username	boolean	true	No	Set to true to disallow the user name in the password.
p_disallow_reverse	boolean	true	No	Set to true to disallow the reverse of the user name in the password.
p_disallow_db_name	boolean	true	No	Set to true to disallow the database or server name in the password.
p_disallow_simple_string	boolean	true	No	Set to true to disallow simple strings as the password.
p_disallow_whitespace	boolean	false	No	Set to true to disallow white space characters in the password.
p_disallow_at_sign	boolean	false	No	Set to true to disallow the @ character in the password.

You can create multiple password verification functions.

There are restrictions on the name of your custom function. Your custom function can't have the same name as an existing system object. The name can be no more than 30 characters long. Also, the name must include one of the following strings: PASSWORD, VERIFY, COMPLEXITY, ENFORCE, or STRENGTH.

The following example creates a function named CUSTOM_PASSWORD_FUNCTION. The function requires that a password has at least 12 characters, 2 uppercase characters, 1 digit, and 1 special character, and that the password disallows the @ character.

```
begin
    rdsadmin.rdsadmin_password_verify.create_verify_function(
        p_verify_function_name => 'CUSTOM_PASSWORD_FUNCTION',
        p_min_length          => 12,
        p_min_uppercase        => 2,
        p_min_digits           => 1,
        p_min_special          => 1,
        p_disallow_at_sign     => true);
end;
/
```

To see the text of your verification function, query DBA_SOURCE. The following example gets the text of a custom password function named CUSTOM_PASSWORD_FUNCTION.

```
COL TEXT FORMAT a150
SELECT TEXT
  FROM DBA_SOURCE
 WHERE OWNER = 'SYS'
```

```
AND NAME = 'CUSTOM_PASSWORD_FUNCTION'
ORDER BY LINE;
```

To associate your verification function with a user profile, use `ALTER PROFILE`. The following example associates a verification function with the `DEFAULT` user profile.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

To see what user profiles are associated with what verification functions, query `DBA_PROFILES`. The following example gets the profiles that are associated with the custom verification function named `CUSTOM_PASSWORD_FUNCTION`.

```
SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD' AND LIMIT =
'CUSTOM_PASSWORD_FUNCTION';
```

PROFILE	RESOURCE_NAME	RESOURCE LIMIT
-----	-----	-----
DEFAULT	PASSWORD_VERIFY_FUNCTION	PASSWORD
CUSTOM_PASSWORD_FUNCTION		

The following example gets all profiles and the password verification functions that they are associated with.

```
SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD_VERIFY_FUNCTION';

PROFILE          RESOURCE_NAME          RESOURCE LIMIT
-----           -----                  -----
DEFAULT          PASSWORD_VERIFY_FUNCTION      PASSWORD
CUSTOM_PASSWORD_FUNCTION
RDSADMIN          PASSWORD_VERIFY_FUNCTION      PASSWORD    NULL
```

[The `create_passthrough_verify_fcn` procedure](#)

The `create_passthrough_verify_fcn` procedure is supported for version 12.1.0.2.v7 and all higher major and minor versions of RDS for Oracle.

You can create a custom function to verify passwords by using the Amazon RDS procedure `rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn`. The `create_passthrough_verify_fcn` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_verify_function_name	varchar2	—	Yes	The name for your custom verification function. This is a wrapper function that is created for you in the <code>SYS</code> schema, and it doesn't contain any verification logic. You assign this function to user profiles.
p_target_owner	varchar2	—	Yes	The schema owner for your custom verification function.

Parameter name	Data type	Default	Required	Description
p_target_function_name	varchar2	—	Yes	The name of your existing custom function that contains the verification logic. Your custom function must return a boolean. Your function should return <code>true</code> if the password is valid and <code>false</code> if the password is invalid.

The following example creates a password verification function that uses the logic from the function named `PASSWORD_LOGIC_EXTRA_STRONG`.

```
begin
    rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn(
        p_verify_function_name => 'CUSTOM_PASSWORD_FUNCTION',
        p_target_owner          => 'TEST_USER',
        p_target_function_name  => 'PASSWORD_LOGIC_EXTRA_STRONG');
end;
/
```

To associate the verification function with a user profile, use `alter profile`. The following example associates the verification function with the `DEFAULT` user profile.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

Setting up a custom DNS server

Amazon RDS supports outbound network access on your DB instances running Oracle. For more information about outbound network access, including prerequisites, see [Configuring UTL_HTTP access using certificates and an Oracle wallet \(p. 1513\)](#).

Amazon RDS Oracle allows Domain Name Service (DNS) resolution from a custom DNS server owned by the customer. You can resolve only fully qualified domain names from your Amazon RDS DB instance through your custom DNS server.

After you set up your custom DNS name server, it takes up to 30 minutes to propagate the changes to your DB instance. After the changes are propagated to your DB instance, all outbound network traffic requiring a DNS lookup queries your DNS server over port 53.

To set up a custom DNS server for your Amazon RDS for Oracle DB instance, do the following:

- From the DHCP options set attached to your virtual private cloud (VPC), set the `domain-name-servers` option to the IP address of your DNS name server. For more information, see [DHCP options sets](#).

Note

The `domain-name-servers` option accepts up to four values, but your Amazon RDS DB instance uses only the first value.

- Ensure that your DNS server can resolve all lookup queries, including public DNS names, Amazon EC2 private DNS names, and customer-specific DNS names. If the outbound network traffic contains any DNS lookups that your DNS server can't handle, your DNS server must have appropriate upstream DNS providers configured.
- Configure your DNS server to produce User Datagram Protocol (UDP) responses of 512 bytes or less.

- Configure your DNS server to produce Transmission Control Protocol (TCP) responses of 1024 bytes or less.
- Configure your DNS server to allow inbound traffic from your Amazon RDS DB instances over port 53. If your DNS server is in an Amazon VPC, the VPC must have a security group that contains inbound rules that permit UDP and TCP traffic on port 53. If your DNS server is not in an Amazon VPC, it must have appropriate firewall allow-listing to permit UDP and TCP inbound traffic on port 53.

For more information, see [Security groups for your VPC](#) and [Adding and removing rules](#).

- Configure the VPC of your Amazon RDS DB instance to allow outbound traffic over port 53. Your VPC must have a security group that contains outbound rules that allow UDP and TCP traffic on port 53.

For more information, see [Security groups for your VPC](#) and [Adding and removing rules](#).

- The routing path between the Amazon RDS DB instance and the DNS server has to be configured correctly to allow DNS traffic.
 - If the Amazon RDS DB instance and the DNS server are not in the same VPC, a peering connection has to be set up between them. For more information, see [What is VPC peering?](#)

Setting and unsetting system diagnostic events

To set and unset diagnostic events at the session level, you can use the Oracle SQL statement `ALTER SESSION SET EVENTS`. However, to set events at the system level you can't use Oracle SQL. Instead, use the system event procedures in the `rdsadmin.rdsadmin_util` package. The system event procedures are available in the following engine versions:

- All Oracle Database 21c versions
- 19.0.0.0.ru-2020-10.rur-2020-10.r1 and higher Oracle Database 19c versions

For more information, see [Version 19.0.0.0.ru-2020-10.rur-2020-10.r1](#) in the *Amazon RDS for Oracle Release Notes*.

- 12.2.0.1.ru-2020-10.rur-2020-10.r1 and higher Oracle Database 12c Release 2 (12.2.0.1) versions

For more information, see [Version 12.2.0.1.ru-2020-10.rur-2020-10.r1](#) in the *Amazon RDS for Oracle Release Notes*.

- 12.1.0.2.V22 and higher Oracle Database 12c Release 1 (12.1.0.2) versions

For more information, see [Version 12.1.0.2.v22](#) in the *Amazon RDS for Oracle Release Notes*.

para

Important

Internally, the `rdsadmin.rdsadmin_util` package sets events by using the `ALTER SYSTEM SET EVENTS` statement. This `ALTER SYSTEM` statement isn't documented in the Oracle Database documentation. Some system diagnostic events can generate large amounts of tracing information, cause contention, or affect database availability. We recommend that you test specific diagnostic events in your nonproduction database, and only set events in your production database under guidance of Oracle Support.

Listing allowed system diagnostic events

To list the system events that you can set, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.list_allowed_system_events`. This procedure accepts no parameters.

The following example lists all system events that you can set.

```
SET SERVEROUTPUT ON
```

```
EXEC rdsadmin.rdsadmin_util.list_allowed_system_events;
```

The following sample output lists event numbers and their descriptions. Use the Amazon RDS procedures `set_system_event` to set these events and `unset_system_event` to unset them.

```

604 - error occurred at recursive SQL level
942 - table or view does not exist
1401 - inserted value too large for column
1403 - no data found
1410 - invalid ROWID
1422 - exact fetch returns more than requested number of rows
1426 - numeric overflow
1427 - single-row subquery returns more than one row
1476 - divisor is equal to zero
1483 - invalid length for DATE or NUMBER bind variable
1489 - result of string concatenation is too long
1652 - unable to extend temp segment by in tablespace
1858 - a non-numeric character was found where a numeric was expected
4031 - unable to allocate bytes of shared memory ("","","","","")
6502 - PL/SQL: numeric or value error
10027 - Specify Deadlock Trace Information to be Dumped
10046 - enable SQL statement timing
10053 - CBO Enable optimizer trace
10173 - Dynamic Sampling time-out error
10442 - enable trace of kst for ORA-01555 diagnostics
12008 - error in materialized view refresh path
12012 - error on auto execute of job
12504 - TNS:listener was not given the SERVICE_NAME in CONNECT_DATA
14400 - inserted partition key does not map to any partition
31693 - Table data object failed to load/unload and is being skipped due to error:
```

Note

The list of the allowed system events can change over time. To make sure that you have the most recent list of eligible events, use `rdsadmin.rdsadmin_util.list_allowed_system_events`.

Setting system diagnostic events

To set a system event, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.set_system_event`. You can only set events listed in the output of `rdsadmin.rdsadmin_util.list_allowed_system_events`. The `set_system_event` procedure accepts the following parameters.

Parameter name	Data type	Default	Required	Description
p_event	number	—	Yes	The system event number. The value must be one of the event numbers reported by <code>list_allowed_system_events</code> .
p_level	number	—	Yes	The event level. See the Oracle Database documentation or Oracle Support for descriptions of different level values.

The procedure `set_system_event` constructs and runs the required `ALTER SYSTEM SET EVENTS` statements according to the following principles:

- The event type (context or errorstack) is determined automatically.
- A statement in the form ALTER SYSTEM SET EVENTS '*event* LEVEL *event_level*' sets the context events. This notation is equivalent to ALTER SYSTEM SET EVENTS '*event* TRACE NAME CONTEXT FOREVER, LEVEL *event_level*'.
- A statement in the form ALTER SYSTEM SET EVENTS '*event* ERRORSTACK (*event_level*)' sets the error stack events. This notation is equivalent to ALTER SYSTEM SET EVENTS '*event* TRACE NAME ERRORSTACK LEVEL *event_level*'.

The following example sets event 942 at level 3, and event 10442 at level 10. Sample output is included.

```
SQL> SET SERVEROUTPUT ON
SQL> EXEC rdsadmin.rdsadmin_util.set_system_event(942,3);
Setting system event 942 with: alter system set events '942 errorstack (3)'

PL/SQL procedure successfully completed.

SQL> EXEC rdsadmin.rdsadmin_util.set_system_event(10442,10);
Setting system event 10442 with: alter system set events '10442 level 10'

PL/SQL procedure successfully completed.
```

[Listing system diagnostic events that are set](#)

To list the system events that are currently set, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.list_set_system_events`. This procedure reports only events set at system level by `set_system_event`.

The following example lists the active system events.

```
SET SERVEROUTPUT ON
EXEC rdsadmin.rdsadmin_util.list_set_system_events;
```

The following sample output shows the list of events, the event type, the level at which the events are currently set, and the time when the event was set.

```
942 errorstack (3) - set at 2020-11-03 11:42:27
10442 level 10 - set at 2020-11-03 11:42:41

PL/SQL procedure successfully completed.
```

[Unsetting system diagnostic events](#)

To unset a system event, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.unset_system_event`. You can only unset events listed in the output of `rdsadmin.rdsadmin_util.list_allowed_system_events`. The `unset_system_event` procedure accepts the following parameter.

Parameter name	Data type	Default	Required	Description
p_event	number	—	Yes	The system event number. The value must be one of the event numbers reported by <code>list_allowed_system_events</code> .

The following example unsets events 942 and 10442. Sample output is included.

```
SQL> SET SERVEROUTPUT ON
SQL> EXEC rdsadmin.rdsadmin_util.unset_system_event(942);
Unsetting system event 942 with: alter system set events '942 off'
PL/SQL procedure successfully completed.

SQL> EXEC rdsadmin.rdsadmin_util.unset_system_event(10442);
Unsetting system event 10442 with: alter system set events '10442 off'
PL/SQL procedure successfully completed.
```

Performing common database tasks for Oracle DB instances

Following, you can find how to perform certain common DBA tasks related to databases on your Amazon RDS DB instances running Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. Amazon RDS also restricts access to some system procedures and tables that require advanced privileges.

Topics

- [Changing the global name of a database \(p. 1543\)](#)
- [Creating and sizing tablespaces \(p. 1544\)](#)
- [Setting the default tablespace \(p. 1544\)](#)
- [Setting the default temporary tablespace \(p. 1545\)](#)
- [Creating a temporary tablespace on the instance store \(p. 1545\)](#)
- [Adding a tempfile to the instance store on a read replica \(p. 1545\)](#)
- [Dropping tempfiles on a read replica \(p. 1546\)](#)
- [Checkpointing a database \(p. 1547\)](#)
- [Setting distributed recovery \(p. 1547\)](#)
- [Setting the database time zone \(p. 1547\)](#)
- [Working with Oracle external tables \(p. 1548\)](#)
- [Generating performance reports with Automatic Workload Repository \(AWR\) \(p. 1549\)](#)
- [Adjusting database links for use with DB instances in a VPC \(p. 1553\)](#)
- [Setting the default edition for a DB instance \(p. 1553\)](#)
- [Enabling auditing for the SYS.AUD\\$ table \(p. 1553\)](#)
- [Disabling auditing for the SYS.AUD\\$ table \(p. 1554\)](#)
- [Cleaning up interrupted online index builds \(p. 1554\)](#)
- [Skipping corrupt blocks \(p. 1555\)](#)
- [Resizing the temporary tablespace in a read replica \(p. 1557\)](#)
- [Purging the recycle bin \(p. 1558\)](#)
- [Setting the Data Redaction policy for full redaction \(p. 1558\)](#)

Changing the global name of a database

To change the global name of a database, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.rename_global_name`. The `rename_global_name` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_new_global_name	varchar2	—	Yes	The new global name for the database.

The database must be open for the name change to occur. For more information about changing the global name of a database, see [ALTER DATABASE](#) in the Oracle documentation.

The following example changes the global name of a database to new_global_name.

```
EXEC rdsadmin.rdsadmin_util.rename_global_name(p_new_global_name => 'new_global_name');
```

Creating and sizing tablespaces

Amazon RDS only supports Oracle Managed Files (OMF) for data files, log files, and control files. When you create data files and log files, you can't specify the physical file names.

By default, tablespaces are created with auto-extend enabled, and no maximum size. Because of these default settings, tablespaces can grow to consume all allocated storage. We recommend that you specify an appropriate maximum size on permanent and temporary tablespaces, and that you carefully monitor space usage.

The following example creates a tablespace named users2 with a starting size of 1 gigabyte and a maximum size of 10 gigabytes:

```
CREATE TABLESPACE users2 DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE 10G;
```

The following example creates temporary tablespace named temp01:

```
CREATE TEMPORARY TABLESPACE temp01;
```

We recommend that you don't use smallfile tablespaces because you can't resize smallfile tablespaces with Amazon RDS for Oracle. However, you can add a datafile to a smallfile tablespace.

You can resize a bigfile tablespace by using `ALTER TABLESPACE`. You can specify the size in kilobytes (K), megabytes (M), gigabytes (G), or terabytes (T).

The following example resizes a bigfile tablespace named users2 to 200 MB.

```
ALTER TABLESPACE users2 RESIZE 200M;
```

The following example adds an additional datafile to a smallfile tablespace named users2.

```
ALTER TABLESPACE users2 ADD DATAFILE SIZE 100000M AUTOEXTEND ON NEXT 250M
MAXSIZE UNLIMITED;
```

Setting the default tablespace

To set the default tablespace, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.alter_default_tablespace`. The `alter_default_tablespace` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
tablespace_name	varchar	—	Yes	The name of the default tablespace.

The following example sets the default tablespace to `users2`:

```
EXEC rdsadmin.rdsadmin_util.alter_default_tablespace(tablespace_name => 'users2');
```

Setting the default temporary tablespace

To set the default temporary tablespace, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.alter_default_temp_tablespace`. The `alter_default_temp_tablespace` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
tablespace_name	varchar	—	Yes	The name of the default temporary tablespace.

The following example sets the default temporary tablespace to `temp01`.

```
EXEC rdsadmin.rdsadmin_util.alter_default_temp_tablespace(tablespace_name => 'temp01');
```

Creating a temporary tablespace on the instance store

To create a temporary tablespace on the instance store, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace`. The `create_inst_store_tmp_tblspace` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_tablespace_name	varchar	—	Yes	The name of the temporary tablespace.

The following example creates the temporary tablespace `temp01` in the instance store.

```
EXEC rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace(p_tablespace_name => 'temp01');
```

Important

When you run `rdsadmin_util.create_inst_store_tmp_tblspace`, the newly created temporary tablespace is not automatically set as the default temporary tablespace. To set it as the default, see [Setting the default temporary tablespace \(p. 1545\)](#).

For more information, see [Storing temporary data in an RDS for Oracle instance store \(p. 1604\)](#).

Adding a tempfile to the instance store on a read replica

When you create a temporary tablespace on a primary DB instance, the read replica doesn't create tempfiles. Assume that an empty temporary tablespace exists on your read replica for either of the following reasons:

- You dropped a tempfile from the tablespace on your read replica. For more information, see [Dropping tempfiles on a read replica \(p. 1546\)](#).
- You created a new temporary tablespace on the primary DB instance. In this case, RDS for Oracle synchronizes the metadata to the read replica.

You can add a tempfile to the empty temporary tablespace, and store the tempfile in the instance store. To create a tempfile in the instance store, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.add_inst_store_tempfile`. You can use this procedure only on a read replica. The procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_tablespace_name</code>	varchar	—	Yes	The name of the temporary tablespace on your read replica.

In the following example, the empty temporary tablespace `temp01` exists on your read replica. Run the following command to create a tempfile for this tablespace, and store it in the instance store.

```
EXEC rdsadmin.rdsadmin_util.add_inst_store_tempfile(p_tablespace_name => 'temp01');
```

For more information, see [Storing temporary data in an RDS for Oracle instance store \(p. 1604\)](#).

Dropping tempfiles on a read replica

You can't drop an existing temporary tablespace on a read replica. You can change the tempfile storage on a read replica from Amazon EBS to the instance store, or from the instance store to Amazon EBS. To achieve these goals, do the following:

1. Drop the current tempfiles in the temporary tablespace on the read replica.
2. Create new tempfiles on different storage.

To drop the tempfiles, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.drop_replica_tempfiles`. You can use this procedure only on read replicas. The `drop_replica_tempfiles` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_tablespace_name</code>	varchar	—	Yes	The name of the temporary tablespace on your read replica.

Assume that a temporary tablespace named `temp01` resides in the instance store on your read replica. Drop all tempfiles in this tablespace by running the following command.

```
EXEC rdsadmin.rdsadmin_util.drop_replica_tempfiles(p_tablespace_name => 'temp01');
```

For more information, see [Storing temporary data in an RDS for Oracle instance store \(p. 1604\)](#).

Checkpointing a database

To checkpoint the database, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.checkpoint`. The checkpoint procedure has no parameters.

The following example checkpoints the database.

```
EXEC rdsadmin.rdsadmin_util.checkpoint;
```

Setting distributed recovery

To set distributed recovery, use the Amazon RDS procedures `rdsadmin.rdsadmin_util.enable_distr_recovery` and `disable_distr_recovery`. The procedures have no parameters.

The following example enables distributed recovery.

```
EXEC rdsadmin.rdsadmin_util.enable_distr_recovery;
```

The following example disables distributed recovery.

```
EXEC rdsadmin.rdsadmin_util.disable_distr_recovery;
```

Setting the database time zone

You can set the time zone of your Amazon RDS Oracle database in the following ways:

- The Timezone option

The Timezone option changes the time zone at the host level and affects all date columns and values such as SYSDATE. For more information, see [Oracle time zone \(p. 1742\)](#).

- The Amazon RDS procedure `rdsadmin.rdsadmin_util.alter_db_time_zone`

The `alter_db_time_zone` procedure changes the time zone for only certain data types, and doesn't change SYSDATE. There are additional restrictions on setting the time zone listed in the [Oracle documentation](#).

Note

You can also set the default time zone for Oracle Scheduler. For more information, see [Setting the time zone for Oracle Scheduler jobs \(p. 1587\)](#).

The `alter_db_time_zone` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_new_tz</code>	varchar2	—	Yes	The new time zone as a named region or an absolute offset from Coordinated Universal Time (UTC). Valid offsets range from -12:00 to +14:00.

The following example changes the time zone to UTC plus three hours.

```
EXEC rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => '+3:00');
```

The following example changes the time zone to the Africa/Algiers time zone.

```
EXEC rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => 'Africa/Algiers');
```

After you alter the time zone by using the `alter_db_time_zone` procedure, reboot your DB instance for the change to take effect. For more information, see [Rebooting a DB instance \(p. 366\)](#). For information about upgrading time zones, see [Time zone considerations \(p. 1762\)](#).

Working with Oracle external tables

Oracle external tables are tables with data that is not in the database. Instead, the data is in external files that the database can access. By using external tables, you can access data without loading it into the database. For more information about external tables, see [Managing external tables](#) in the Oracle documentation.

With Amazon RDS, you can store external table files in directory objects. You can create a directory object, or you can use one that is predefined in the Oracle database, such as the `DATA_PUMP_DIR` directory. For information about creating directory objects, see [Creating and dropping directories in the main data storage space \(p. 1597\)](#). You can query the `ALL_DIRECTORIES` view to list the directory objects for your Amazon RDS Oracle DB instance.

Note

Directory objects point to the main data storage space (Amazon EBS volume) used by your instance. The space used—along with data files, redo logs, audit, trace, and other files—counts against allocated storage.

You can move an external data file from one Oracle database to another by using the `DBMS_FILE_TRANSFER` package or the `UTL_FILE` package. The external data file is moved from a directory on the source database to the specified directory on the destination database. For information about using `DBMS_FILE_TRANSFER`, see [Importing using Oracle Data Pump \(p. 1616\)](#).

After you move the external data file, you can create an external table with it. The following example creates an external table that uses the `emp_xt_file1.txt` file in the `USER_DIR1` directory.

```
CREATE TABLE emp_xt (
    emp_id      NUMBER,
    first_name  VARCHAR2(50),
    last_name   VARCHAR2(50),
    user_name   VARCHAR2(20)
)
ORGANIZATION EXTERNAL (
    TYPE ORACLE_LOADER
    DEFAULT DIRECTORY USER_DIR1
    ACCESS PARAMETERS (
        RECORDS DELIMITED BY NEWLINE
        FIELDS TERMINATED BY ','
        MISSING FIELD VALUES ARE NULL
        (emp_id,first_name,last_name,user_name)
    )
    LOCATION ('emp_xt_file1.txt')
)
PARALLEL
REJECT LIMIT UNLIMITED;
```

Suppose that you want to move data that is in an Amazon RDS Oracle DB instance into an external data file. In this case, you can populate the external data file by creating an external table and selecting the

data from the table in the database. For example, the following SQL statement creates the `orders_xt` external table by querying the `orders` table in the database.

```
CREATE TABLE orders_xt
ORGANIZATION EXTERNAL
(
    TYPE ORACLE_DATAPUMP
    DEFAULT DIRECTORY DATA_PUMP_DIR
    LOCATION ('orders_xt.dmp')
)
AS SELECT * FROM orders;
```

In this example, the data is populated in the `orders_xt.dmp` file in the `DATA_PUMP_DIR` directory.

Generating performance reports with Automatic Workload Repository (AWR)

To gather performance data and generate reports, Oracle recommends Automatic Workload Repository (AWR). AWR requires Oracle Database Enterprise Edition and a license for the Diagnostics and Tuning packs. To enable AWR, set the `CONTROL_MANAGEMENT_PACK_ACCESS` initialization parameter to either `DIAGNOSTIC` or `DIAGNOSTIC+TUNING`.

Working with AWR reports in RDS

To generate AWR reports, you can run scripts such as `awrrpt.sql`. These scripts are installed on the database host server. In Amazon RDS, you don't have direct access to the host. However, you can get copies of SQL scripts from another installation of Oracle Database.

You can also use AWR by running procedures in the `SYS.DBMS_WORKLOAD_REPOSITORY` PL/SQL package. You can use this package to manage baselines and snapshots, and also to display ASH and AWR reports. For example, to generate an AWR report in text format run the `DBMS_WORKLOAD_REPOSITORY.AWR_REPORT_TEXT` procedure. However, you can't reach these AWR reports from the AWS Management Console.

When working with AWR, we recommend using the `rdsadmin.rdsadmin_diagnostic_util` procedures. You can use these procedures to generate the following:

- AWR reports
- Active Session History (ASH) reports
- Automatic Database Diagnostic Monitor (ADDM) reports
- Oracle Data Pump Export dump files of AWR data

The `rdsadmin_diagnostic_util` procedures save the reports to the DB instance file system. You can access these reports from the console. You can also access reports using the `rdsadmin.rds_file_util` procedures, and you can access reports that are copied to Amazon S3 using the S3 Integration option. For more information, see [Reading files in a DB instance directory \(p. 1598\)](#) and [Amazon S3 integration \(p. 1648\)](#).

You can use the `rdsadmin_diagnostic_util` procedures in the following Amazon RDS for Oracle DB engine versions:

- All Oracle Database 21c versions
- 19.0.0.0.ru-2020-04.rur-2020-04.r1 and higher Oracle Database 19c versions
- 12.2.0.1.ru-2020-04.rur-2020-04.r1 and higher Oracle Database 12c Release 2 (12.2) versions
- 12.1.0.2.v20 and higher Oracle Database 12c Release 1 (12.1) versions

Common parameters for the diagnostic utility package

You typically use the following parameters when managing AWR and ADDM with the `rdsadmin_diagnostic_util` package.

Parameter	Data type	Default	Requires	Description
<code>begin_snap_id</code>	NUMBER	—	Yes	The ID of the beginning snapshot.
<code>end_snap_id</code>	NUMBER	—	Yes	The ID of the ending snapshot.
<code>dump_directory</code>	VARCHAR2	RDDUMP	No	The directory to write the report or export file to. If you specify a nondefault directory, the user that runs the <code>rdsadmin_diagnostic_util</code> procedures must have write permissions for the directory.
<code>p_tag</code>	VARCHAR2	—	No	<p>A string that can be used to distinguish between backups to indicate the purpose or usage of backups, such as incremental or daily.</p> <p>You can specify up to 30 characters. Valid characters are a-z, A-Z, 0-9, an underscore (_), a dash (-), and a period (.). The tag is not case-sensitive. RMAN always stores tags in uppercase, regardless of the case used when entering them.</p> <p>Tags don't need to be unique, so multiple backups can have the same tag. If you don't specify a tag, RMAN assigns a default tag automatically using the format <code>TAGYYYYMMDDTHHMMSS</code>, where <code>YYYY</code> is the year, <code>MM</code> is the month, <code>DD</code> is the day, <code>HH</code> is the hour (in 24-hour format), <code>MM</code> is the minutes, and <code>SS</code> is the seconds. The date and time indicate when RMAN started the backup. For example, a backup with the default tag <code>TAG20190927T214517</code> indicates a backup that started on 2019-09-27 at 21:45:17.</p> <p>The <code>p_tag</code> parameter is supported for the following RDS for Oracle DB engine versions:</p> <ul style="list-style-type: none"> • Oracle Database 21c (21.0.0) • Oracle Database 19c (19.0.0), using 19.0.0.ru-2021-10.rur-2021-10.r1 and higher • Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2021-10.rur-2021-10.r1 and higher • Oracle Database 12c Release 1 (12.1), using 12.1.0.2.V26 and higher
<code>report_type</code>	VARCHAR2	HTML	No	The format of the report. Valid values are TEXT and HTML.
<code>dbid</code>	NUMBER	—	No	A valid database identifier (DBID) shown in the <code>DBA_HIST_DATABASE_INSTANCE</code> view for Oracle. If this parameter is not specified, RDS uses the current DBID, which is shown in the <code>V\$DATABASE.DBID</code> view.

You typically use the following parameters when managing ASH with the `rdsadmin_diagnostic_util` package.

Parameter	Data type	Default	Require	Description
begin_time	DATE	—	Yes	The beginning time of the ASH analysis.
end_time	DATE	—	Yes	The ending time of the ASH analysis.
slot_width	NUMBER	0	No	The duration of the slots (in seconds) used in the "Top Activity" section of the ASH report. If this parameter isn't specified, the time interval between begin_time and end_time uses no more than 10 slots.
sid	NUMBER	Null	No	The session ID.
sql_id	VARCHAR2	Null	No	The SQL ID.
wait_class	VARCHAR2	Null	No	The wait class name.
service_hash	NUMBER	Null	No	The service name hash.
module_name	VARCHAR2	Null	No	The module name.
action_name	VARCHAR2	Null	No	The action name.
client_id	VARCHAR2	Null	No	The application-specific ID of the database session.
plsql_entry	VARCHAR2	Null	No	The PL/SQL entry point.

Generating an AWR report

To generate an AWR report, use the `rdsadmin.rdsadmin_diagnostic_util.awr_report` procedure.

The following example generates a AWR report for the snapshot range 101–106. The output text file is named `awrrpt_101_106.txt`. You can access this report from the AWS Management Console.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_report(101,106,'TEXT');
```

The following example generates an HTML report for the snapshot range 63–65. The output HTML file is named `awrrpt_63_65.html`. The procedure writes the report to the nondefault database directory named `AWR_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_report(63,65,'HTML','AWR_RPT_DUMP');
```

Extracting AWR data into a dump file

To extract AWR data into a dump file, use the `rdsadmin.rdsadmin_diagnostic_util.awr_extract` procedure.

The following example extracts the snapshot range 101–106. The output dump file is named `awrextract_101_106.dmp`. You can access this file through the console.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_extract(101,106);
```

The following example extracts the snapshot range 63–65. The output dump file is named `awrextract_63_65.dmp`. The file is stored in the nondefault database directory named `AWR_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_extract(63,65,'AWR_RPT_DUMP');
```

Generating an ADDM report

To generate an ADDM report, use the `rdsadmin.rdsadmin_diagnostic_util.addm_report` procedure.

The following example generates an ADDM report for the snapshot range 101–106. The output text file is named `addmrpt_101_106.txt`. You can access the report through the console.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.addm_report(101,106);
```

The following example generates an ADDM report for the snapshot range 63–65. The output text file is named `addmrpt_63_65.txt`. The file is stored in the nondefault database directory named `ADDM_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.addm_report(63,65,'ADDM_RPT_DUMP');
```

Generating an ASH report

To generate an ASH report, use the `rdsadmin.rdsadmin_diagnostic_util.ash_report` procedure.

The following example generates an ASH report that includes the data from 14 minutes ago until the current time. The name of the output file uses the format `ashrptbegin_timeend_time.txt`, where `begin_time` and `end_time` use the format YYYYMMDDHH24MISS. You can access the file through the console.

```
BEGIN
    rdsadmin.rdsadmin_diagnostic_util.ash_report(
        begin_time      =>      SYSDATE-14/1440,
        end_time        =>      SYSDATE,
        report_type     =>      'TEXT');
END;
/
```

The following example generates an ASH report that includes the data from November 18, 2019, at 6:07 PM through November 18, 2019, at 6:15 PM. The name of the output HTML report is `ashrpt_20190918180700_20190918181500.html`. The report is stored in the nondefault database directory named `AWR_RPT_DUMP`.

```
BEGIN
    rdsadmin.rdsadmin_diagnostic_util.ash_report(
        begin_time      =>      TO_DATE('2019-09-18 18:07:00', 'YYYY-MM-DD HH24:MI:SS'),
        end_time        =>      TO_DATE('2019-09-18 18:15:00', 'YYYY-MM-DD HH24:MI:SS'),
        report_type     =>      'html',
        dump_directory  =>      'AWR_RPT_DUMP');
END;
/
```

Accessing AWR reports from the console or CLI

To access AWR reports or export dump files, you can use the AWS Management Console or AWS CLI. For more information, see [Downloading a database log file \(p. 681\)](#).

Adjusting database links for use with DB instances in a VPC

To use Oracle database links with Amazon RDS DB instances inside the same virtual private cloud (VPC) or peered VPCs, the two DB instances should have a valid route between them. Verify the valid route between the DB instances by using your VPC routing tables and network access control list (ACL).

The security group of each DB instance must allow ingress to and egress from the other DB instance. The inbound and outbound rules can refer to security groups from the same VPC or a peered VPC. For more information, see [Updating your security groups to reference peered VPC security groups](#).

If you have configured a custom DNS server using the DHCP Option Sets in your VPC, your custom DNS server must be able to resolve the name of the database link target. For more information, see [Setting up a custom DNS server \(p. 1539\)](#).

For more information about using database links with Oracle Data Pump, see [Importing using Oracle Data Pump \(p. 1616\)](#).

Setting the default edition for a DB instance

You can redefine database objects in a private environment called an edition. You can use edition-based redefinition to upgrade an application's database objects with minimal downtime.

You can set the default edition of an Amazon RDS Oracle DB instance using the Amazon RDS procedure `rdsadmin.rdsadmin_util.alter_default_edition`.

The following example sets the default edition for the Amazon RDS Oracle DB instance to RELEASE_V1.

```
EXEC rdsadmin.rdsadmin_util.alter_default_edition('RELEASE_V1');
```

The following example sets the default edition for the Amazon RDS Oracle DB instance back to the Oracle default.

```
EXEC rdsadmin.rdsadmin_util.alter_default_edition('ORA$BASE');
```

For more information about Oracle edition-based redefinition, see [About editions and edition-based redefinition](#) in the Oracle documentation.

Enabling auditing for the SYS.AUD\$ table

To enable auditing on the database audit trail table SYS.AUD\$, use the Amazon RDS procedure `rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table`. The only supported audit property is ALL. You can't audit or not audit individual statements or operations.

Enabling auditing is supported for Oracle DB instances running the following versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1.0.2.v14) and later

The `audit_all_sys_aud_table` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_by_access	boolean	true	No	Set to true to audit BY ACCESS. Set to false to audit BY SESSION.

Note

In a single-tenant CDB, the following operations work, but no customer-visible mechanism can detect the current status of the operations. Auditing information isn't available from within the PDB. For more information, see [Limitations of a single-tenant CDB \(p. 1486\)](#).

The following query returns the current audit configuration for SYS.AUD\$ for a database.

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

The following commands enable audit of ALL on SYS.AUD\$ BY ACCESS.

```
EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table;
EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table(p_by_access => true);
```

The following command enables audit of ALL on SYS.AUD\$ BY SESSION.

```
EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table(p_by_access => false);
```

For more information, see [AUDIT \(traditional auditing\)](#) in the Oracle documentation.

Disabling auditing for the SYS.AUD\$ table

To disable auditing on the database audit trail table SYS.AUD\$, use the Amazon RDS procedure `rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table`. This procedure takes no parameters.

The following query returns the current audit configuration for SYS.AUD\$ for a database:

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

The following command disables audit of ALL on SYS.AUD\$.

```
EXEC rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table;
```

For more information, see [NOAUDIT \(traditional auditing\)](#) in the Oracle documentation.

Cleaning up interrupted online index builds

To clean up failed online index builds, use the Amazon RDS procedure `rdsadmin.rdsadmin_dbms_repair.online_index_clean`.

The `online_index_clean` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
object_id	binary_integer	ALL_INDEX_ID	No	The object ID of the index. Typically, you can use

Parameter name	Data type	Default	Required	Description
				the object ID from the ORA-08104 error text.
wait_for_lock	binary_integer	rdsadmin.rdsadmin_dbms_repair.lock_nowait	\$ADMIN_DBMS_REPAIR_WAITFORLOCK	Specify <code>rdsadmin.rdsadmin_dbms_repair.lock_nowait</code> to try to get a lock on the underlying object and retry until an internal limit is reached if the lock fails. Specify <code>rdsadmin.rdsadmin_dbms_repair.lock_noretry</code> to try to get a lock on the underlying object but not retry if the lock fails.

The following example cleans up a failed online index build:

```

declare
    is_clean boolean;
begin
    is_clean := rdsadmin.rdsadmin_dbms_repair.online_index_clean(
        object_id      => 1234567890,
        wait_for_lock => rdsadmin.rdsadmin_dbms_repair.lock_nowait
    );
end;
/

```

For more information, see [ONLINE_INDEX_CLEAN function](#) in the Oracle documentation.

Skipping corrupt blocks

To skip corrupt blocks during index and table scans, use the `rdsadmin.rdsadmin_dbms_repair` package.

The following procedures wrap the functionality of the `sys.dbms_repair.admin_table` procedure and take no parameters:

- `rdsadmin.rdsadmin_dbms_repair.create_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.create_orphan_keys_table`
- `rdsadmin.rdsadmin_dbms_repair.drop_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.drop_orphan_keys_table`
- `rdsadmin.rdsadmin_dbms_repair.purge_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.purge_orphan_keys_table`

The following procedures take the same parameters as their counterparts in the `DBMS_REPAIR` package for Oracle databases:

- `rdsadmin.rdsadmin_dbms_repair.check_object`
- `rdsadmin.rdsadmin_dbms_repair.dump_orphan_keys`
- `rdsadmin.rdsadmin_dbms_repair.fix_corrupt_blocks`
- `rdsadmin.rdsadmin_dbms_repair.rebuild_freelists`

- `rdsadmin.rdsadmin_dbms_repair.segment_fix_status`
- `rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks`

For more information about handling database corruption, see [DBMS_REPAIR](#) in the Oracle documentation.

Example Responding to corrupt blocks

This example shows the basic workflow for responding to corrupt blocks. Your steps will depend on the location and nature of your block corruption.

Important

Before attempting to repair corrupt blocks, review the [DBMS_REPAIR](#) documentation carefully.

To skip corrupt blocks during index and table scans

1. Run the following procedures to create repair tables if they don't already exist.

```
EXEC rdsadmin.rdsadmin_dbms_repair.create_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.create_orphan_keys_table;
```

2. Run the following procedures to check for existing records and purge them if appropriate.

```
SELECT COUNT(*) FROM SYS.REPAIR_TABLE;
SELECT COUNT(*) FROM SYS.ORPHAN_KEY_TABLE;
SELECT COUNT(*) FROM SYS.DBA_REPAIR_TABLE;
SELECT COUNT(*) FROM SYS.DBA_ORPHAN_KEY_TABLE;

EXEC rdsadmin.rdsadmin_dbms_repair.purge_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.purge_orphan_keys_table;
```

3. Run the following procedure to check for corrupt blocks.

```
SET SERVEROUTPUT ON
DECLARE v_num_corrupt INT;
BEGIN
    v_num_corrupt := 0;
    rdsadmin.rdsadmin_dbms_repair.check_object (
        schema_name => '&corruptionOwner',
        object_name => '&corruptionTable',
        corrupt_count => v_num_corrupt
    );
    dbms_output.put_line('number corrupt: '||to_char(v_num_corrupt));
END;
/

COL CORRUPT_DESCRIPTION FORMAT a30
COL REPAIR_DESCRIPTION FORMAT a30

SELECT OBJECT_NAME, BLOCK_ID, CORRUPT_TYPE, MARKED_CORRUPT,
       CORRUPT_DESCRIPTION, REPAIR_DESCRIPTION
  FROM   SYS.REPAIR_TABLE;

SELECT SKIP_CORRUPT
  FROM   DBA_TABLES
 WHERE  OWNER = '&corruptionOwner'
 AND    TABLE_NAME = '&corruptionTable';
```

4. Use the `skip_corrupt_blocks` procedure to enable or disable corruption skipping for affected tables. Depending on the situation, you may also need to extract data to a new table, and then drop the table containing the corrupt block.

Run the following procedure to enable corruption skipping for affected tables.

```

begin
    rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks (
        schema_name => '&corruptionOwner',
        object_name => '&corruptionTable',
        object_type => rdsadmin.rdsadmin_dbms_repair.table_object,
        flags => rdsadmin.rdsadmin_dbms_repair.skip_flag);
end;
/
select skip_corrupt from dba_tables where owner = '&corruptionOwner' and table_name =
    '&corruptionTable';

```

Run the following procedure to disable corruption skipping.

```

begin
    rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks (
        schema_name => '&corruptionOwner',
        object_name => '&corruptionTable',
        object_type => rdsadmin.rdsadmin_dbms_repair.table_object,
        flags => rdsadmin.rdsadmin_dbms_repair.noskip_flag);
end;
/
select skip_corrupt from dba_tables where owner = '&corruptionOwner' and table_name =
    '&corruptionTable';

```

5. When you have completed all repair work, run the following procedures to drop the repair tables.

```

EXEC rdsadmin.rdsadmin_dbms_repair.drop_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.drop_orphan_keys_table;

```

Resizing the temporary tablespace in a read replica

By default, Oracle tablespaces are created with auto-extend enabled and no maximum size. Because of these default settings, tablespaces can grow too large in some cases. We recommend that you specify an appropriate maximum size on permanent and temporary tablespaces, and that you carefully monitor space usage.

To resize the temporary space in a read replica for an Oracle DB instance, use either the `rdsadmin.rdsadmin_util.resize_temp_tablespace` or the `rdsadmin.rdsadmin_util.resize_tempfile` Amazon RDS procedure.

The `resize_temp_tablespace` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>temp_tbs</code>	varchar2	—	Yes	The name of the temporary tablespace to resize.
<code>size</code>	varchar2	—	Yes	You can specify the size in bytes (the default), kilobytes (K), megabytes (M), or gigabytes (G).

The `resize_tempfile` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
file_id	binary_integer	—	Yes	The file identifier of the temporary tablespace to resize.
size	varchar2	—	Yes	You can specify the size in bytes (the default), kilobytes (K), megabytes (M), or gigabytes (G).

The following examples resize a temporary tablespace named TEMP to the size of 4 gigabytes on a read replica.

```
EXEC rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP', '4G');
```

```
EXEC rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP', '4096000000');
```

The following example resizes a temporary tablespace based on the tempfile with the file identifier 1 to the size of 2 megabytes on a read replica.

```
EXEC rdsadmin.rdsadmin_util.resize_tempfile(1, '2M');
```

For more information about read replicas for Oracle DB instances, see [Working with read replicas for Amazon RDS for Oracle \(p. 1630\)](#).

Purging the recycle bin

When you drop a table, your Oracle database doesn't immediately remove its storage space. The database renames the table and places it and any associated objects in a recycle bin. Purging the recycle bin removes these items and releases their storage space.

To purge the entire recycle bin, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.purge_dba_recyclebin`. However, this procedure can't purge the recycle bin of SYS and RDSADMIN objects. If you need to purge these objects, contact AWS Support.

The following example purges the entire recycle bin.

```
EXEC rdsadmin.rdsadmin_util.purge_dba_recyclebin;
```

Setting the Data Redaction policy for full redaction

To change the default displayed values for a Data Redaction policy for full redaction on your Amazon RDS Oracle instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val`.

The `dbms_redact_upd_full_rdct_val` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_number_val	number	Null	No	Modifies the default value for columns of the NUMBER datatype.

Parameter name	Data type	Default	Required	Description
p_binfloor_val	binary_float	Null	No	Modifies the default value for columns of the BINARY_FLOAT datatype.
p_bindouble_val	binary_double	Null	No	Modifies the default value for columns of the BINARY_DOUBLE datatype.
p_char_val	char	Null	No	Modifies the default value for columns of the CHAR datatype.
p_varchar_val	varchar2	Null	No	Modifies the default value for columns of the VARCHAR2 datatype.
p_nchar_val	nchar	Null	No	Modifies the default value for columns of the NCHAR datatype.
p_nvarchar_val	nvarchar2	Null	No	Modifies the default value for columns of the NVARCHAR2 datatype.
p_date_val	date	Null	No	Modifies the default value for columns of the DATE datatype.
p_ts_val	timestamp	Null	No	Modifies the default value for columns of the TIMESTAMP datatype.
p_tswtz_val	timestamp with time zone	Null	No	Modifies the default value for columns of the TIMESTAMP WITH TIME ZONE datatype.
p_blob_val	blob	Null	No	Modifies the default value for columns of the BLOB datatype.
p_clob_val	clob	Null	No	Modifies the default value for columns of the CLOB datatype.
p_nclob_val	nclob	Null	No	Modifies the default value for columns of the NCLOB datatype.

The following example changes the default redacted value to * for char datatype:

```
EXEC rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val(p_char_val => '*');
```

The following example changes the default redacted values for number, date and char datatypes:

```
begin
```

```
rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val(  
    p_number_val=>1,  
    p_date_val=>to_date('1900-01-01', 'YYYY-MM-DD'),  
    p_varchar_val=>'X');  
end;  
/
```

After you alter the default values for full redaction with the dbms_redact_upd_full_rdct_val procedure, reboot your DB instance for the change to take effect. For more information, see [Rebooting a DB instance \(p. 366\)](#).

Performing common log-related tasks for Oracle DB instances

Following, you can find how to perform certain common DBA tasks related to logging on your Amazon RDS DB instances running Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances, and restricts access to certain system procedures and tables that require advanced privileges.

For more information, see [Oracle database log files \(p. 709\)](#).

Topics

- [Setting force logging \(p. 1560\)](#)
- [Setting supplemental logging \(p. 1561\)](#)
- [Switching online log files \(p. 1561\)](#)
- [Adding online redo logs \(p. 1562\)](#)
- [Dropping online redo logs \(p. 1562\)](#)
- [Resizing online redo logs \(p. 1563\)](#)
- [Retaining archived redo logs \(p. 1564\)](#)
- [Accessing online and archived redo logs \(p. 1566\)](#)
- [Downloading archived redo logs from Amazon S3 \(p. 1566\)](#)

Setting force logging

In force logging mode, Oracle logs all changes to the database except changes in temporary tablespaces and temporary segments (NOLANDING clauses are ignored). For more information, see [Specifying FORCE LOGGING mode](#) in the Oracle documentation.

To set force logging, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.force_logging`. The `force_logging` procedure has the following parameters.

Parameter name	Data type	Default	Yes	Description
p_enable	boolean	true	No	Set to true to put the database in force logging mode, false to remove the database from force logging mode.

The following example puts the database in force logging mode.

```
EXEC rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

Setting supplemental logging

If you enable supplemental logging, LogMiner has the necessary information to support chained rows and clustered tables. For more information, see [Supplemental logging](#) in the Oracle documentation.

Oracle Database doesn't enable supplemental logging by default. To enable and disable supplemental logging, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.alter_supplemental_logging`. For more information about how Amazon RDS manages the retention of archived redo logs for Oracle DB instances, see [Retaining archived redo logs \(p. 1564\)](#).

The `alter_supplemental_logging` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_action</code>	<code>varchar2</code>	—	Yes	'ADD' to add supplemental logging, 'DROP' to drop supplemental logging.
<code>p_type</code>	<code>varchar2</code>	<code>null</code>	No	The type of supplemental logging. Valid values are 'ALL', 'FOREIGN KEY', 'PRIMARY KEY', 'UNIQUE', or PROCEDURAL.

The following example enables supplemental logging.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD');
end;
/
```

The following example enables supplemental logging for all fixed-length maximum size columns.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'ALL');
end;
/
```

The following example enables supplemental logging for primary key columns.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'PRIMARY KEY');
end;
/
```

Switching online log files

To switch log files, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.switch_logfile`. The `switch_logfile` procedure has no parameters.

The following example switches log files.

```
EXEC rdsadmin.rdsadmin_util.switch_logfile;
```

Adding online redo logs

An Amazon RDS DB instance running Oracle starts with four online redo logs, 128 MB each. To add additional redo logs, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.add_logfile`.

The `add_logfile` procedure has the following parameters.

Note

The parameters are mutually exclusive.

Parameter name	Data type	Default	Required	Description
bytes	positive	null	No	The size of the log file in bytes.
p_size	varchar2	—	Yes	The size of the log file. You can specify the size in kilobytes (K), megabytes (M), or gigabytes (G).

The following command adds a 100 MB log file.

```
EXEC rdsadmin.rdsadmin_util.add_logfile(p_size => '100M');
```

Dropping online redo logs

To drop redo logs, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.drop_logfile`. The `drop_logfile` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
grp	positive	—	Yes	The group number of the log.

The following example drops the log with group number 3.

```
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 3);
```

You can only drop logs that have a status of unused or inactive. The following example gets the statuses of the logs.

```
SELECT GROUP#, STATUS FROM V$LOG;  
  
GROUP#      STATUS  
-----  
1           CURRENT  
2           INACTIVE  
3           INACTIVE
```

4 UNUSED

Resizing online redo logs

An Amazon RDS DB instance running Oracle starts with four online redo logs, 128 MB each. The following example shows how you can use Amazon RDS procedures to resize your logs from 128 MB each to 512 MB each.

```
/* Query V$LOG to see the logs.          */
/* You start with 4 logs of 128 MB each. */

SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#    BYTES      STATUS
----- -----
1         134217728  INACTIVE
2         134217728  CURRENT
3         134217728  INACTIVE
4         134217728  INACTIVE

/* Add four new logs that are each 512 MB */

EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);

/* Query V$LOG to see the logs. */
/* Now there are 8 logs.        */

SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#    BYTES      STATUS
----- -----
1         134217728  INACTIVE
2         134217728  CURRENT
3         134217728  INACTIVE
4         134217728  INACTIVE
5         536870912   UNUSED
6         536870912   UNUSED
7         536870912   UNUSED
8         536870912   UNUSED

/* Drop each inactive log using the group number. */

EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 1);
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 3);
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 4);

/* Query V$LOG to see the logs. */
/* Now there are 5 logs.        */

select GROUP#, BYTES, STATUS from V$LOG;

GROUP#    BYTES      STATUS
----- -----
2         134217728  CURRENT
5         536870912   UNUSED
6         536870912   UNUSED
7         536870912   UNUSED
```

```

8          536870912  UNUSED

/* Switch logs so that group 2 is no longer current. */

EXEC rdsadmin.rdsadmin_util.switch_logfile;

/* Query V$LOG to see the logs.      */
/* Now one of the new logs is current. */

SQL>SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
----- -----
2          134217728  ACTIVE
5          536870912  CURRENT
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED

/* If the status of log 2 is still "ACTIVE", issue a checkpoint to clear it to "INACTIVE".
 */

EXEC rdsadmin.rdsadmin_util.checkpoint;

/* Query V$LOG to see the logs.      */
/* Now the final original log is inactive. */

select GROUP#, BYTES, STATUS from V$LOG;

GROUP#     BYTES      STATUS
----- -----
2          134217728  INACTIVE
5          536870912  CURRENT
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED

# Drop the final inactive log.

EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 2);

/* Query V$LOG to see the logs.      */
/* Now there are four 512 MB logs. */

SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
----- -----
5          536870912  CURRENT
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED

```

Retaining archived redo logs

You can retain archived redo logs locally on your DB instance for use with products like Oracle LogMiner (DBMS_LOGMNR). After you have retained the redo logs, you can use LogMiner to analyze the logs. For more information, see [Using LogMiner to analyze redo log files](#) in the Oracle documentation.

To retain archived redo logs, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.set_configuration`. The `set_configuration` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
name	varchar	—	Yes	The name of the configuration to update.
value	varchar	—	Yes	The value for the configuration.

The following example retains 24 hours of redo logs.

```
begin
    rdsadmin.rdsadmin_util.set_configuration(
        name  => 'archivelog retention hours',
        value => '24');
end;
/
commit;
```

Note

The commit is required for the change to take effect.

To view how long archived redo logs are kept for your DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.show_configuration`.

The following example shows the log retention time.

```
set serveroutput on
EXEC rdsadmin.rdsadmin_util.show_configuration;
```

The output shows the current setting for `archivelog retention hours`. The following output shows that archived redo logs are kept for 48 hours.

```
NAME:archivelog retention hours
VALUE:48
DESCRIPTION:ArchiveLog expiration specifies the duration in hours before archive/redo log files are automatically deleted.
```

Because the archived redo logs are retained on your DB instance, ensure that your DB instance has enough allocated storage for the retained logs. To determine how much space your DB instance has used in the last X hours, you can run the following query, replacing X with the number of hours.

```
SELECT SUM(BLOCKS * BLOCK_SIZE) bytes
  FROM V$ARCHIVED_LOG
 WHERE FIRST_TIME >= SYSDATE-(X/24) AND DEST_ID=1;
```

RDS for Oracle only generates archived redo logs when the backup retention period of your DB instance is greater than zero. By default the backup retention period is greater than zero.

When the archived log retention period expires, RDS for Oracle removes the archived redo logs from your DB instance. To support restoring your DB instance to a point in time, Amazon RDS retains the archived redo logs outside of your DB instance based on the backup retention period. To modify the backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

In some cases, you might be using JDBC on Linux to download archived redo logs and experience long latency times and connection resets. In such cases, the issues might be caused by the default random number generator setting on your Java client. We recommend setting your JDBC drivers to use a nonblocking random number generator.

Accessing online and archived redo logs

You might want to access your online and archived redo log files for mining with external tools such as GoldenGate, Attunity, Informatica, and others. To access these files, do the following:

1. Create directory objects that provide read-only access to the physical file paths.

Use `rdsadmin.rdsadmin_master_util.create_archivelog_dir` and `rdsadmin.rdsadmin_master_util.create_onlinelog_dir`.

2. Read the files using PL/SQL.

You can read the files by using PL/SQL. For more information about reading files from directory objects, see [Listing files in a DB instance directory \(p. 1598\)](#) and [Reading files in a DB instance directory \(p. 1598\)](#).

Accessing transaction logs is supported for the following releases:

- Oracle Database 21c
- Oracle Database 19c
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1)

The following code creates directories that provide read-only access to your online and archived redo log files:

Important

This code also revokes the `DROP ANY DIRECTORY` privilege.

```
EXEC rdsadmin.rdsadmin_master_util.create_archivelog_dir;
EXEC rdsadmin.rdsadmin_master_util.create_onlinelog_dir;
```

The following code drops the directories for your online and archived redo log files.

```
EXEC rdsadmin.rdsadmin_master_util.drop_archivelog_dir;
EXEC rdsadmin.rdsadmin_master_util.drop_onlinelog_dir;
```

The following code grants and revokes the `DROP ANY DIRECTORY` privilege.

```
EXEC rdsadmin.rdsadmin_master_util.revoke_drop_any_directory;
EXEC rdsadmin.rdsadmin_master_util.grant_drop_any_directory;
```

Downloading archived redo logs from Amazon S3

You can download archived redo logs on your DB instance using the `rdsadmin.rdsadmin_archive_log_download` package. If archived redo logs are no longer on your DB instance, you might want to download them again from Amazon S3. Then you can mine the logs or use them to recover or replicate your database.

Note

You can't download archived redo logs on read replica instances.

Downloading archived redo logs: basic steps

The availability of your archived redo logs depends on the following retention policies:

- Backup retention policy – Logs inside of this policy are available in Amazon S3. Logs outside of this policy are removed.
- Archived log retention policy – Logs inside of this policy are available on your DB instance. Logs outside of this policy are removed.

If logs aren't on your instance but are protected by your backup retention period, use `rdsadmin.rdsadmin_archive_log_download` to download them again. RDS for Oracle saves the logs to the `/rdsdbdata/log/arch` directory on your DB instance.

To download archived redo logs from Amazon S3

1. Increase your archived redo log retention period so that RDS won't delete the logs that you download. Make sure to COMMIT your change.
To learn how to set the retention policy, see [Retaining archived redo logs \(p. 1564\)](#).
2. Wait up to 5 minutes for the archived log retention policy change to take effect.
3. Download the archived redo logs from Amazon S3 using `rdsadmin.rdsadmin_archive_log_download`.

For more information, see [Downloading a single archived redo log \(p. 1567\)](#) and [Downloading a series of archived redo logs \(p. 1568\)](#).

Note

RDS automatically checks the available storage before downloading. If the requested logs consume a high percentage of space, you receive an alert.

4. Confirm that the logs were downloaded from Amazon S3 successfully.

You can view the status of your download task in a bdump file. The bdump files have the path name `/rdsdbdata/log/trace/dbtask-task-id.log`. In the preceding download step, you run a SELECT statement that returns the task ID in a VARCHAR2 data type. For more information, see similar examples in [Monitoring the status of a file transfer \(p. 1662\)](#).

Downloading a single archived redo log

To download a single archived redo log to the `/rdsdbdata/log/arch` directory, use `rdsadmin.rdsadmin_archive_log_download.download_log_with_seqnum`. This procedure has the following parameter.

Parameter name	Data type	Default	Required	Description
seqnum	number	—	Yes	The sequence number of the archived redo log.

The following example downloads the log with sequence number 20.

```
SELECT rdsadmin.rdsadmin_archive_log_download.download_log_with_seqnum(seqnum => 20)
      AS TASK_ID
  FROM DUAL;
```

Downloading a series of archived redo logs

To download a series of archived redo logs to the /rdsdbdata/log/arch directory, use `download_logs_in_seqnum_range`. Your download is limited to 300 logs per request. The `download_logs_in_seqnum_range` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>start_seq</code>	number	—	Yes	The starting sequence number for the series.
<code>end_seq</code>	number	—	Yes	The ending sequence number for the series.

The following example downloads the logs from sequence 50 to 100.

```
SELECT rdsadmin.rdsadmin_archive_log_download.download_logs_in_seqnum_range(start_seq =>
50, end_seq => 100)
      AS TASK_ID
FROM   DUAL;
```

Performing common RMAN tasks for Oracle DB instances

In the following section, you can find how you can perform Oracle Recovery Manager (RMAN) DBA tasks on your Amazon RDS DB instances running Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances. It also restricts access to certain system procedures and tables that require advanced privileges.

You can use the Amazon RDS package `rdsadmin.rdsadmin_rman_util` to perform RMAN backups of your Amazon RDS for Oracle database to disk. The `rdsadmin.rdsadmin_rman_util` package supports full and incremental database file backups, tablespace backups, and archive log backups.

RMAN backups consume storage space on the Amazon RDS DB instance host. When you perform a backup, you specify an Oracle directory object as a parameter in the procedure call. The backup files are placed in the specified directory. You can use default directories, such as `DATA_PUMP_DIR`, or create a new directory. For more information, see [Creating and dropping directories in the main data storage space \(p. 1597\)](#).

After an RMAN backup has finished, you can copy the backup files off the Amazon RDS for Oracle DB instance host. You might do this for the purpose of restoring to a non-RDS host or for long-term storage of backups. For example, you can copy the backup files to an Amazon S3 bucket. For more information, see using [Amazon S3 integration \(p. 1648\)](#).

The backup files for RMAN backups remain on the Amazon RDS DB instance host until you remove them manually. You can use the `UTL_FILE.FREMOVE` Oracle procedure to remove files from a directory. For more information, see [FREMOVE procedure](#) in the Oracle documentation.

When backing up archived redo logs or performing a full or incremental backup that includes archived redo logs, redo log retention must be set to a nonzero value. For more information, see [Retaining archived redo logs \(p. 1564\)](#).

Note

For backing up and restoring to another Amazon RDS for Oracle DB instance, you can continue to use the Amazon RDS backup and restore features. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#)

Currently, RMAN restore isn't supported for Amazon RDS for Oracle DB instances.

Topics

- [Common parameters for RMAN procedures \(p. 1569\)](#)
- [Validating DB instance files \(p. 1571\)](#)
- [Enabling and disabling block change tracking \(p. 1574\)](#)
- [Crosschecking archived redo logs \(p. 1575\)](#)
- [Backing up archived redo logs \(p. 1576\)](#)
- [Performing a full database backup \(p. 1581\)](#)
- [Performing an incremental database backup \(p. 1582\)](#)
- [Backing up a tablespace \(p. 1583\)](#)
- [Backing up a control file \(p. 1584\)](#)

Common parameters for RMAN procedures

You can use procedures in the Amazon RDS package `rdsadmin.rdsadmin_rman_util` to perform tasks with RMAN. Several parameters are common to the procedures in the package. The package has the following common parameters.

Parameter name	Data type	Valid values	Default	Required	Description
p_directory_name	varchar2	A valid database directory name.	—	Yes	The name of the directory to contain the backup files.
p_label	varchar2	a-z, A-Z, 0-9, '_', '-', '.'	—	No	A unique string that is included in the backup file names. Note The limit is 30 characters.
p_owner	varchar2	A valid owner of the directory specified in p_directory_name.	—	Yes	The owner of the directory to contain the backup files.
p_tag	varchar2	a-z, A-Z, 0-9, '_', '-', '.'	NULL	No	A string that can be used to distinguish between backups to indicate the purpose or usage of backups, such as daily, weekly, or incremental-level backups. The limit is 30 characters. The tag is not case-sensitive. Tags are always stored in uppercase, regardless of the case used when entering them. Tags don't need to be unique, so multiple backups can have the same tag. If you don't specify a tag, then RMAN assigns a default tag automatically using the format TAGYYYYMMDDTHHMMSS, where YYYY is the year, MM is the month, DD is the day, HH is the hour (in 24-hour format), MM is the minutes,

Parameter name	Data type	Valid values	Default	Required	Description
					<p>and <i>SS</i> is the seconds. The date and time refer to when RMAN started the backup.</p> <p>For example, a backup might receive a tag TAG20190927T214517 for a backup that started on 2019-09-27 at 21:45:17.</p> <p>The p_tag parameter is supported for the following Amazon RDS for Oracle DB engine versions:</p> <ul style="list-style-type: none"> • Oracle Database 21c (21.0.0) • Oracle Database 19c (19.0.0), using 19.0.0.0.ru-2021-10.rur-2021-10.r1 or higher • Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2021-10.rur-2021-10.r1 or higher • Oracle Database 12c Release 1 (12.1), using 12.1.0.2.V26 or higher
p_compress	boolean	TRUE, FALSE	FALSE	No	<p>Specify TRUE to enable BASIC backup compression.</p> <p>Specify FALSE to disable BASIC backup compression.</p>
p_include_archived_logs	boolean	TRUE, FALSE	FALSE	No	<p>Specify TRUE to include archived redo logs in the backup.</p> <p>Specify FALSE to exclude archived redo logs from the backup.</p> <p>If you include archived redo logs in the backup, set retention to one hour or greater using the <code>rdsadmin.rdsadmin_util.set_configuration</code> procedure. Also, call the <code>rdsadmin.rdsadmin_rman_util.crosscheck_archive</code> procedure immediately before running the backup. Otherwise, the backup might fail due to missing archived redo log files that have been deleted by Amazon RDS management procedures.</p>
p_include_controlfile	boolean	TRUE, FALSE	FALSE	No	<p>Specify TRUE to include the control file in the backup.</p> <p>Specify FALSE to exclude the control file from the backup.</p>
p_optimize	boolean	TRUE, FALSE	TRUE	No	<p>Specify TRUE to enable backup optimization, if archived redo logs are included, to reduce backup size.</p> <p>Specify FALSE to disable backup optimization.</p>

Parameter name	Data type	Valid values	Default	Required	Description
p_parallel	number	A valid integer between 1 and 254 for Oracle Database Enterprise Edition (EE) 1 for other Oracle Database editions	1	No	Number of channels.
p_rman_to_dbms_output	boolean	TRUE, FALSE	FALSE	No	When TRUE, the RMAN output is sent to the DBMS_OUTPUT package in addition to a file in the BDUMP directory. In SQL*Plus, use SET SERVEROUTPUT ON to see the output. When FALSE, the RMAN output is only sent to a file in the BDUMP directory.
p_section_size_mb	number	A valid integer	NULL	No	The section size in megabytes (MB). Validates in parallel by dividing each file into the specified section size. When NULL, the parameter is ignored.
p_validation_type	varchar2	'PHYSICAL', 'PHYSICAL+LOGICAL'	'PHYSICAL'		The level of corruption detection. Specify 'PHYSICAL' to check for physical corruption. An example of physical corruption is a block with a mismatch in the header and footer. Specify 'PHYSICAL+LOGICAL' to check for logical inconsistencies in addition to physical corruption. An example of logical corruption is a corrupt block.

Validating DB instance files

You can use the Amazon RDS package `rdsadmin.rdsadmin_rman_util` to validate Amazon RDS for Oracle DB instance files, such as data files, tablespaces, control files, or server parameter files (SPFILEs).

For more information about RMAN validation, see [Validating database files and backups](#) and [VALIDATE](#) in the Oracle documentation.

Topics

- [Validating a DB instance \(p. 1572\)](#)
- [Validating a tablespace \(p. 1572\)](#)
- [Validating a control file \(p. 1573\)](#)
- [Validating an SPFILE \(p. 1573\)](#)

- [Validating a data file \(p. 1573\)](#)

Validating a DB instance

To validate all of the relevant files used by an Amazon RDS Oracle DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.validate_database`.

This procedure uses the following common parameters for RMAN tasks:

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

The following example validates the DB instance using the default values for the parameters.

```
EXEC rdsadmin.rdsadmin_rman_util.validate_database;
```

The following example validates the DB instance using the specified values for the parameters.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.validate_database(
        p_validation_type      => 'PHYSICAL+LOGICAL',
        p_parallel             => 4,
        p_section_size_mb     => 10,
        p_rman_to_dbms_output => FALSE);
END;
/
```

When the `p_rman_to_dbms_output` parameter is set to FALSE, the RMAN output is written to a file in the BDUMP directory.

To view the files in the BDUMP directory, run the following SELECT statement.

```
SELECT * FROM table(rdsadmin.rds_file_util.listdir('BDUMP')) order by mtime;
```

To view the contents of a file in the BDUMP directory, run the following SELECT statement.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','rds-rman-
validate-nnn.txt'));
```

Replace the file name with the name of the file you want to view.

Validating a tablespace

To validate the files associated with a tablespace, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.validate_tablespace`.

This procedure uses the following common parameters for RMAN tasks:

- `p_validation_type`
- `p_parallel`

- p_section_size_mb
- p_rman_to_dbms_output

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameter.

Parameter name	Data type	Valid values	Default	Required	Description
p_tablespace_name	varchar2	A valid tablespace name	—	Yes	The name of the tablespace.

Validating a control file

To validate only the control file used by an Amazon RDS Oracle DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.validate_current_controlfile`.

This procedure uses the following common parameter for RMAN tasks:

- p_validation_type
- p_rman_to_dbms_output

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

Validating an SPFILE

To validate only the server parameter file (SPFILE) used by an Amazon RDS Oracle DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.validate_spfile`.

This procedure uses the following common parameter for RMAN tasks:

- p_validation_type
- p_rman_to_dbms_output

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

Validating a data file

To validate a data file, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.validate_datafile`.

This procedure uses the following common parameters for RMAN tasks:

- p_validation_type
- p_parallel
- p_section_size_mb
- p_rman_to_dbms_output

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameters.

Parameter name	Data type	Valid values	Default	Required	Description
p_datafile	varchar2	A valid datafile ID number or a valid datafile name including complete path	—	Yes	The datafile ID number (from v \$datafile.file#) or the full datafile name including the path (from v \$datafile.name).
p_from_block	number	A valid integer	NULL	No	The number of the block where the validation starts within the data file. When this is NULL, 1 is used.
p_to_block	number	A valid integer	NULL	No	The number of the block where the validation ends within the data file. When this is NULL, the maximum block in the data file is used.

Enabling and disabling block change tracking

Block changing tracking records changed blocks in a tracking file. This technique can improve the performance of RMAN incremental backups. For more information, see [Using Block Change Tracking to Improve Incremental Backup Performance](#) in the Oracle Database documentation.

To enable block change tracking for a DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.enable_block_change_tracking`. To disable block change tracking, use `disable_block_change_tracking`. These procedures take no parameters.

Read-only replicas support block change tracking. If you create a read-only replica from a source DB that uses block change tracking, the replica uses block change tracking. You can't enable block change tracking on a mounted replica. If you place a mounted replica in read-only mode, block change tracking isn't enabled, but you can enable it using `enable_block_change_tracking`. If you promote an Oracle replica to a source DB, you can use block change tracking just as for any other Oracle DB instance.

Block change tracking procedures are supported for the following DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

Note

In a single-tenant CDB, the following operations work, but no customer-visible mechanism can detect the current status of the operations. See also [Limitations of a single-tenant CDB \(p. 1486\)](#).

To determine whether block change tracking is enabled for your DB instance, run the following query.

```
SELECT STATUS, FILENAME FROM V$BLOCK_CHANGE_TRACKING;
```

The following example enables block change tracking for a DB instance.

```
EXEC rdsadmin.rdsadmin_rman_util.enable_block_change_tracking;
```

The following example disables block change tracking for a DB instance.

```
EXEC rdsadmin.rdsadmin_rman_util.disable_block_change_tracking;
```

Crosschecking archived redo logs

You can crosscheck archived redo logs using the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.crosscheck_archivelog`.

You can use this procedure to crosscheck the archived redo logs registered in the control file and optionally delete the expired logs records. When RMAN makes a backup, it creates a record in the control file. Over time, these records increase the size of the control file. We recommend that you remove expired records periodically.

Note

Standard Amazon RDS backups don't use RMAN and therefore don't create records in the control file.

This procedure uses the common parameter `p_rman_to_dbms_output` for RMAN tasks.

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameter.

Parameter name	Data type	Valid values	Default	Required	Description
<code>p_delete_expired</code>	boolean	TRUE, FALSE	TRUE	No	<p>When TRUE, delete expired archived redo log records from the control file.</p> <p>When FALSE, retain the expired archived redo log records in the control file.</p>

This procedure is supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

The following example marks archived redo log records in the control file as expired, but does not delete the records.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => FALSE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

The following example deletes expired archived redo log records from the control file.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => TRUE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Backing up archived redo logs

You can use the Amazon RDS package `rdsadmin.rdsadmin_rman_util` to back up archived redo logs for an Amazon RDS Oracle DB instance.

The procedures for backing up archived redo logs are supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

Topics

- [Backing up all archived redo logs \(p. 1576\)](#)
- [Backing up an archived redo log from a date range \(p. 1577\)](#)
- [Backing up an archived redo log from an SCN range \(p. 1578\)](#)
- [Backing up an archived redo log from a sequence number range \(p. 1580\)](#)

Backing up all archived redo logs

To back up all of the archived redo logs for an Amazon RDS Oracle DB instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_archivelog_all`.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

The following example backs up all archived redo logs for the DB instance.

```

BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_all(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_parallel       => 4,
        p_tag            => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/

```

Backing up an archived redo log from a date range

To back up specific archived redo logs for an Amazon RDS Oracle DB instance by specifying a date range, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_archivelog_date`. The date range specifies which archived redo logs to back up.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameters.

Parameter name	Data type	Valid values	Default	Required	Description
<code>p_from_date</code>	date	A date that is between the <code>start_date</code> and <code>next_date</code> of an archived redo log that exists on disk. The value must be less than or equal to the value	—	Yes	The starting date for the archived log backups.

Parameter name	Data type	Valid values	Default	Required	Description
		specified for p_to_date.			
p_to_date	date	A date that is between the start_date and next_date of an archived redo log that exists on disk. The value must be greater than or equal to the value specified for p_from_date.	—	Yes	The ending date for the archived log backups.

The following example backs up archived redo logs in the date range for the DB instance.

```

BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_date(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_from_date      => '03/01/2019 00:00:00',
        p_to_date        => '03/02/2019 00:00:00',
        p_parallel       => 4,
        p_tag            => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/

```

Backing up an archived redo log from an SCN range

To back up specific archived redo logs for an Amazon RDS Oracle DB instance by specifying a system change number (SCN) range, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_archivelog_scn`. The SCN range specifies which archived redo logs to back up.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`

- p_parallel
- p_compress
- p_rman_to_dbms_output
- p_tag

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameters.

Parameter name	Data type	Valid values	Default	Required	Description
p_from_scn	number	An SCN of an archived redo log that exists on disk. The value must be less than or equal to the value specified for p_to_scn.	—	Yes	The starting SCN for the archived log backups.
p_to_scn	number	An SCN of an archived redo log that exists on disk. The value must be greater than or equal to the value specified for p_from_scn.	—	Yes	The ending SCN for the archived log backups.

The following example backs up archived redo logs in the SCN range for the DB instance.

```

BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_scn(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_from_scn       => 1533835,
        p_to_scn         => 1892447,
        p_parallel       => 4,
        p_tag            => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);

```

```
END;
/
```

Backing up an archived redo log from a sequence number range

To back up specific archived redo logs for an Amazon RDS Oracle DB instance by specifying a sequence number range, use the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_archivelog_sequence`. The sequence number range specifies which archived redo logs to back up.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameters.

Parameter name	Data type	Valid values	Default	Required	Description
<code>p_from_sequence</code>	number	A sequence number of an archived redo log that exists on disk. The value must be less than or equal to the value specified for <code>p_to_sequence</code> .	—	Yes	The starting sequence number for the archived log backups.
<code>p_to_sequence</code>	number	A sequence number of an archived redo log that exists on disk. The value must be	—	Yes	The ending sequence number for the archived log backups.

Parameter name	Data type	Valid values	Default	Required	Description
		greater than or equal to the value specified for p_from_sequence.			

The following example backs up archived redo logs in the sequence number range for the DB instance.

```

BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_sequence(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_from_sequence  => 11160,
        p_to_sequence    => 11160,
        p_parallel       => 4,
        p_tag            => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/

```

Performing a full database backup

You can perform a backup of all blocks of data files included in the backup using Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_database_full`.

This procedure uses the following common parameters for RMAN tasks:

- p_owner
- p_directory_name
- p_label
- p_parallel
- p_section_size_mb
- p_include_archive_logs
- p_optimize
- p_compress
- p_rman_to_dbms_output
- p_tag

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure is supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

The following example performs a full backup of the DB instance using the specified values for the parameters.

```

BEGIN
    rdsadmin.rdsadmin_rman_util.backup_database_full(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_parallel       => 4,
        p_section_size_mb => 10,
        p_tag            => 'FULL_DB_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/

```

Performing an incremental database backup

You can perform an incremental backup of your DB instance using the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_database_incremental`.

For more information about incremental backups, see [Incremental backups](#) in the Oracle documentation.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_include_controlfile`
- `p_optimize`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure is supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

This procedure also uses the following additional parameter.

Parameter name	Data type	Valid values	Default	Required	Description
<code>p_level</code>	number	0, 1	0	No	Specify 0 to enable a full incremental backup.

Parameter name	Data type	Valid values	Default	Required	Description
					Specify 1 to enable a non-cumulative incremental backup.

The following example performs an incremental backup of the DB instance using the specified values for the parameters.

```

BEGIN
    rdsadmin.rdsadmin_xman_util.backup_database_incremental(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_level          => 1,
        p_parallel       => 4,
        p_section_size_mb => 10,
        p_tag            => 'MY_INCREMENTAL_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/

```

Backing up a tablespace

You can back up a tablespace using the Amazon RDS procedure `rdsadmin.rdsadmin_xman_util.backup_tablespace`.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_include_controlfile`
- `p_optimize`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure also uses the following additional parameter.

Parameter name	Data type	Valid values	Default	Required	Description
<code>p_tablespace_name</code>	varchar2	A valid tablespace name.	—	Yes	The name of the tablespace to back up.

This procedure is supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

The following example performs a tablespace backup using the specified values for the parameters.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_tablespace(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_tablespace_name => 'MYTABLESPACE',
        p_parallel        => 4,
        p_section_size_mb => 10,
        p_tag             => 'MYTABLESPACE_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Backing up a control file

You can back up a control file using the Amazon RDS procedure `rdsadmin.rdsadmin_rman_util.backup_current_controlfile`.

This procedure uses the following common parameters for RMAN tasks:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

For more information, see [Common parameters for RMAN procedures \(p. 1569\)](#).

This procedure is supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2), using 12.2.0.1.ru-2019-01.rur-2019-01.r1 or higher
- Oracle Database 12c Release 1 (12.1), using 12.1.0.2.v15 or higher

The following example backs up a control file using the specified values for the parameters.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_tablespace(
        p_owner          => 'SYS',
        p_directory_name => 'MYDIRECTORY',
        p_tag             => 'CONTROL_FILE_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Performing common scheduling tasks for Oracle DB instances

Some scheduler jobs owned by SYS can interfere with normal database operations. Oracle Support recommends you disable these jobs or modify the schedule. To perform tasks for Oracle Scheduler jobs owned by SYS, use the Amazon RDS package `rdsadmin.rdsadmin_dbms_scheduler`.

The `rdsadmin.rdsadmin_dbms_scheduler` procedures are supported for the following Amazon RDS for Oracle DB engine versions:

- Oracle Database 21c (21.0.0)
 - Oracle Database 19c
 - Oracle Database 12c Release 2 (12.2) on 12.2.0.2.ru-2019-07.rur-2019-07.r1 or higher 12.2 versions
 - Oracle Database 12c Release 1 (12.1) on 12.1.0.2.v17 or higher 12.1 versions

Common parameters for Oracle Scheduler procedures

To perform tasks with Oracle Scheduler, use procedures in the Amazon RDS package `rdsadmin.rdsadmin_dbms_scheduler`. Several parameters are common to the procedures in the package. The package has the following common parameters.

Parameter name	Data type	Valid values	Default	Required	Description
name	varchar2	'SYS.BSLN_MAINTAIN_STATS_JOB'	The name of the job to modify.		<p>Note</p> <p>Currently, you can only modify SYS.CLEANUP_ONLINE_IND_BUILD and SYS.BSLN_MAINTAIN_STATS_JOB jobs.</p>
attribute	varchar2	'REPEAT_INTERVAL', 'SCHEUDLE_NAME'	The attribute to modify.		<p>To modify the repeat interval for the job, specify 'REPEAT_INTERVAL'.</p> <p>To modify the schedule name for the job, specify 'SCHEUDLE_NAME'.</p>
value	varchar2	A valid schedule interval or schedule name, depending on	-	Yes	The new value of the attribute.

Parameter name	Data type	Valid values	Default	Required	Description
		attribute used.			

Modifying DBMS_SCHEDULER jobs

To modify certain components of Oracle Scheduler, use the Oracle procedure `dbms_scheduler.set_attribute`. For more information, see [DBMS_SCHEDULER](#) and [SET_ATTRIBUTE procedure](#) in the Oracle documentation.

When working with Amazon RDS DB instances, prepend the schema name SYS to the object name. The following example sets the resource plan attribute for the Monday window object.

```

BEGIN
    DBMS_SCHEDULER.SET_ATTRIBUTE(
        name      => 'SYS.MONDAY_WINDOW',
        attribute => 'RESOURCE_PLAN',
        value     => 'resource_plan_1');
END;
/

```

Modifying AutoTask maintenance windows

Amazon RDS for Oracle instances are created with default settings for maintenance windows. Automated maintenance tasks such as optimizer statistics collection run during these windows. By default, the maintenance windows turn on Oracle Database Resource Manager.

To modify the window, use the DBMS_SCHEDULER package. You might need to modify the maintenance window settings for the following reasons:

- You want maintenance jobs to run at a different time, with different settings, or not at all. For example, might want to modify the window duration, or change the repeat time and interval.
- You want to avoid the performance impact of enabling Resource Manager during maintenance. For example, if the default maintenance plan is specified, and if the maintenance window opens while the database is under load, you might see wait events such as `resmgr:cpu quantum`. This wait event is related to Database Resource Manager. You have the following options:
 - Ensure that maintenance windows are active during off-peak times for your DB instance.
 - Disable the default maintenance plan by setting the `resource_plan` attribute to an empty string.
 - Set the `resource_manager_plan` parameter to `FORCE`: in your parameter group. If your instance uses Enterprise Edition, this setting prevents Database Resource Manager plans from activating.

To modify your maintenance window settings

1. Connect to your database using an Oracle SQL client.
2. Query the current configuration for a scheduler window.

The following example queries the configuration for MONDAY_WINDOW.

```

SELECT ENABLED, RESOURCE_PLAN, DURATION, REPEAT_INTERVAL
FROM   DBA_SCHEDULER_WINDOWS
WHERE  WINDOW_NAME='MONDAY_WINDOW';

```

The following output shows that the window is using the default values.

ENABLED	RESOURCE_PLAN	DURATION	REPEAT_INTERVAL
TRUE	DEFAULT_MAINTENANCE_PLAN freq=daily;byday=MON;byhour=22	+000 04:00:00 ;byminute=0; bysecond=0	

3. Modify the window using the DBMS_SCHEDULER package.

The following example sets the resource plan to null so that the Resource Manager won't run during the maintenance window.

```
BEGIN
    -- disable the window to make changes
    DBMS_SCHEDULER.DISABLE(name=>'SYS"."MONDAY_WINDOW', force=>TRUE);

    -- specify the empty string to use no plan
    DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'SYS"."MONDAY_WINDOW',
        attribute=>'RESOURCE_PLAN', value=>'');

    -- re-enable the window
    DBMS_SCHEDULER.ENABLE(name=>'SYS"."MONDAY_WINDOW');
END;
/
```

The following example sets the maximum duration of the window to 2 hours.

```
BEGIN
    DBMS_SCHEDULER.DISABLE(name=>'SYS"."MONDAY_WINDOW', force=>TRUE);
    DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'SYS"."MONDAY_WINDOW', attribute=>'DURATION',
        value=>'0 2:00:00');
    DBMS_SCHEDULER.ENABLE(name=>'SYS"."MONDAY_WINDOW');
END;
/
```

The following example sets the repeat interval to every Monday at 10 AM.

```
BEGIN
    DBMS_SCHEDULER.DISABLE(name=>'SYS"."MONDAY_WINDOW', force=>TRUE);
    DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'SYS"."MONDAY_WINDOW',
        attribute=>'REPEAT_INTERVAL',
        value=>'freq=daily;byday=MON;byhour=10;byminute=0;bysecond=0');
    DBMS_SCHEDULER.ENABLE(name=>'SYS"."MONDAY_WINDOW');
END;
/
```

Setting the time zone for Oracle Scheduler jobs

To modify the time zone for Oracle Scheduler, you can use the Oracle procedure `dbms_scheduler.set_scheduler_attribute`. For more information about the `dbms_scheduler` package, see [DBMS_SCHEDULER](#) and [SET_SCHEDULER_ATTRIBUTE](#) in the Oracle documentation.

To modify the current time zone setting

1. Connect to the database using a client such as SQL Developer. For more information, see [Connecting to your DB instance using Oracle SQL developer \(p. 1490\)](#).
2. Set the default time zone as following, substituting your time zone for `time_zone_name`.

```
BEGIN
  DBMS_SCHEDULER.SET_SCHEDULER_ATTRIBUTE(
    attribute => 'default_timezone',
    value => 'time_zone_name'
  );
END;
/
```

In the following example, you change the time zone to Asia/Shanghai.

Start by querying the current time zone, as shown following.

```
SELECT VALUE FROM DBA_SCHEDULER_GLOBAL_ATTRIBUTE WHERE ATTRIBUTE_NAME='DEFAULT_TIMEZONE';
```

The output shows that the current time zone is ETC/UTC.

```
VALUE
-----
Etc/UTC
```

Then you set the time zone to Asia/Shanghai.

```
BEGIN
  DBMS_SCHEDULER.SET_SCHEDULER_ATTRIBUTE(
    attribute => 'default_timezone',
    value => 'Asia/Shanghai'
  );
END;
/
```

For more information about changing the system time zone, see [Oracle time zone \(p. 1742\)](#).

Turning off Oracle Scheduler jobs owned by SYS

To disable an Oracle Scheduler job owned by the SYS user, use the `rdsadmin.rdsadmin_dbms_scheduler.disable` procedure.

This procedure uses the `name` common parameter for Oracle Scheduler tasks. For more information, see [Common parameters for Oracle Scheduler procedures \(p. 1585\)](#).

The following example disables the `SYS.CLEANUP_ONLINE_IND_BUILD` Oracle Scheduler job.

```
BEGIN
  rdsadmin.rdsadmin_dbms_scheduler.disable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Turning on Oracle Scheduler jobs owned by SYS

To turn on an Oracle Scheduler job owned by SYS, use the `rdsadmin.rdsadmin_dbms_scheduler.enable` procedure.

This procedure uses the `name` common parameter for Oracle Scheduler tasks. For more information, see [Common parameters for Oracle Scheduler procedures \(p. 1585\)](#).

The following example enables the `SYS.CLEANUP_ONLINE_IND_BUILD` Oracle Scheduler job.

```
BEGIN
    rdsadmin.rdsadmin_dbms_scheduler.enable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Modifying the Oracle Scheduler repeat interval for jobs of CALENDAR type

To modify the repeat interval to modify a SYS-owned Oracle Scheduler job of CALENDAR type, use the `rdsadmin.rdsadmin_dbms_scheduler.disable` procedure.

This procedure uses the following common parameters for Oracle Scheduler tasks:

- `name`
- `attribute`
- `value`

For more information, see [Common parameters for Oracle Scheduler procedures \(p. 1585\)](#).

The following example modifies the repeat interval of the `SYS.CLEANUP_ONLINE_IND_BUILD` Oracle Scheduler job.

```
BEGIN
    rdsadmin.rdsadmin_dbms_scheduler.set_attribute(
        name      => 'SYS.CLEANUP_ONLINE_IND_BUILD',
        attribute => 'repeat_interval',
        value     => 'freq=daily;byday=FRI,SAT;byhour=20;byminute=0;bysecond=0');
END;
/
```

Modifying the Oracle Scheduler repeat interval for jobs of NAMED type

Some Oracle Scheduler jobs use a schedule name instead of an interval. For this type of jobs, you must create a new named schedule in the master user schema. Use the standard `Oracle sys.dbms_scheduler.create_schedule` procedure to do this. Also, use the `rdsadmin.rdsadmin_dbms_scheduler.set_attribute` procedure to assign the new named schedule to the job.

This procedure uses the following common parameter for Oracle Scheduler tasks:

- `name`
- `attribute`
- `value`

For more information, see [Common parameters for Oracle Scheduler procedures \(p. 1585\)](#).

The following example modifies the repeat interval of the `SYS.BSLN_MAINTAIN_STATS_JOB` Oracle Scheduler job.

```
BEGIN
    DBMS_SCHEDULER.CREATE_SCHEDULE (
        schedule_name  => 'rds_master_user.new_schedule',
        start_date     => SYSTIMESTAMP,
```

```

repeat_interval =>
'freq=daily;byday=MON,TUE,WED,THU,FRI;byhour=0;byminute=0;bysecond=0',
end_date      => NULL,
comments       => 'Repeats daily forever');
END;
/
BEGIN
    rdsadmin.rdsadmin_dbms_scheduler.set_attribute (
        name      => 'SYS.BSLN_MAINTAIN_STATS_JOB',
        attribute => 'schedule_name',
        value     => 'rds_master_user.new_schedule');
END;
/

```

Turning off autocommit for Oracle Scheduler job creation

When DBMS_SCHEDULER.CREATE_JOB creates Oracle Scheduler jobs, it creates the jobs immediately and commits the changes. You might need to incorporate the creation of Oracle Scheduler jobs in the user transaction to do the following:

- Roll back the Oracle Schedule job when the user transaction is rolled back.
- Create the Oracle Scheduler job when the main user transaction is committed.

You can use the procedure `rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag` to turn on this behavior. This procedure takes no parameters. You can use this procedure in the following RDS for Oracle releases:

- 21.0.0.0.ru-2022-07.rur-2022-07.r1 and higher
- 19.0.0.0.ru-2022-07.rur-2022-07.r1 and higher

The following example turns off autocommit for Oracle Scheduler, creates an Oracle Scheduler job, and then rolls back the transaction. Because autocommit is turned off, the database also rolls back the creation of the Oracle Scheduler job.

```

BEGIN
    rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag;
    DBMS_SCHEDULER.CREATE_JOB(job_name    => 'EMPTY_JOB',
                               job_type     => 'PLSQL_BLOCK',
                               job_action   => 'begin null; end;',
                               auto_drop   => false);
    ROLLBACK;
END;
/
PL/SQL procedure successfully completed.

SELECT * FROM DBA_SCHEDULER_JOBS WHERE JOB_NAME='EMPTY_JOB';

no rows selected

```

Performing common diagnostic tasks for Oracle DB instances

Oracle Database includes a fault diagnosability infrastructure that you can use to investigate database problems. In Oracle terminology, a *problem* is a critical error such as a code bug or data corruption. An *incident* is the occurrence of a problem. If the same error occurs three times, then the infrastructure

shows three incidents of this problem. For more information, see [Diagnosing and resolving problems](#) in the Oracle Database documentation.

The Automatic Diagnostic Repository Command Interpreter (ADRCI) utility is an Oracle command-line tool that you use to manage diagnostic data. For example, you can use this tool to investigate problems and package diagnostic data. An *incident package* includes diagnostic data for an incident or all incidents that reference a specific problem. You can upload an incident package, which is implemented as a .zip file, to Oracle Support.

To deliver a managed service experience, Amazon RDS doesn't provide shell access to ADRCI. To perform diagnostic tasks for your Oracle instance, instead use the Amazon RDS package `rdsadmin.rdsadmin_adrci_util`.

By using the functions in `rdsadmin_adrci_util`, you can list and package problems and incidents, and also show trace files. All functions return a task ID. This ID forms part of the name of log file that contains the ADRCI output, as in `dbtask-task_id.log`. The log file resides in the BDUMP directory.

Common parameters for diagnostic procedures

To perform diagnostic tasks, use functions in the Amazon RDS package `rdsadmin.rdsadmin_adrci_util`. The package has the following common parameters.

Parameter name	Data type	Valid values	Default	Required	Description
<code>incident_id</code>	number	A valid incident ID or null	Null	No	If the value is null, the function shows all incidents. If the value isn't null and represents a valid incident ID, the function shows the specified incident.
<code>problem_id</code>	number	A valid problem ID or null	Null	No	If the value is null, the function shows all problems. If the value isn't null and represents a valid problem ID, the function shows the specified problem.
<code>last</code>	number	A valid integer greater than 0 or null	Null	No	If the value is null, then the function displays at most 50 items. If the value isn't null, the function displays the specified number.

Listing incidents

To list diagnostic incidents for Oracle, use the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents`. You can list incidents in either basic or detailed mode. By default, the function lists the 50 most recent incidents.

This function uses the following common parameters:

- `incident_id`

- problem_id

If you specify both of the preceding parameters, incident_id overrides problem_id. For more information, see [Common parameters for diagnostic procedures \(p. 1591\)](#).

This function uses the following additional parameter.

Parameter name	Data type	Valid values	Default	Required	Description
detail	boolean	TRUE or FALSE	FALSE	No	If TRUE, the function lists incidents in detail mode. If FALSE, the function lists incidents in basic mode.

To list all incidents, query the rdsadmin.rdsadmin_adrci_util.list_adrci_incidents function without any arguments. The query returns the task ID.

```
SQL> SELECT rdsadmin.rdsadmin_adrci_util.list_adrci_incidents AS task_id FROM DUAL;
TASK_ID
-----
1590786706158-3126
```

Or call the rdsadmin.rdsadmin_adrci_util.list_adrci_incidents function without any arguments and store the output in a SQL client variable. You can use the variable in other statements.

```
SQL> VAR task_id VARCHAR2(80);
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_incidents;
PL/SQL procedure successfully completed.
```

To read the log file, call the Amazon RDS procedure rdsadmin.rds_file_util.read_text_file. Supply the task ID as part of the file name. The following output shows three incidents: 53523, 53522, and 53521.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
'dbtask-'||:task_id||'.log'));

TEXT
-----
2020-05-29 21:11:46.193 UTC [INFO ] Listing ADRCI incidents.
2020-05-29 21:11:46.256 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*****
INCIDENT_ID PROBLEM_KEY CREATE_TIME
-----
53523      ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_003 2020-05-29
20:15:20.928000 +00:00
53522      ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_002 2020-05-29
20:15:15.247000 +00:00
53521      ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_001 2020-05-29
20:15:06.047000 +00:00
3 rows fetched
```

```
2020-05-29 21:11:46.256 UTC [INFO ] The ADRCI incidents were successfully listed.  
2020-05-29 21:11:46.256 UTC [INFO ] The task finished successfully.  
14 rows selected.
```

To list a particular incident, specify its ID using the `incident_id` parameter. In the following example, you query the log file for incident 53523 only.

```
SQL> EXEC :task_id :=  
rdsadmin.rdsadmin_adrci_util.list_adrci_incidents(incident_id=>53523);  
  
PL/SQL procedure successfully completed.  
  
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',  
'dbtask-'||:task_id||'.log'));  
  
TEXT  
-----  
2020-05-29 21:15:25.358 UTC [INFO ] Listing ADRCI incidents.  
2020-05-29 21:15:25.426 UTC [INFO ]  
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:  
*****  
INCIDENT_ID          PROBLEM_KEY  
CREATE_TIME  
-----  
-----  
53523                ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_003 2020-05-29  
20:15:20.928000 +00:00  
1 rows fetched  
  
2020-05-29 21:15:25.427 UTC [INFO ] The ADRCI incidents were successfully listed.  
2020-05-29 21:15:25.427 UTC [INFO ] The task finished successfully.  
12 rows selected.
```

Listing problems

To list diagnostic problems for Oracle, use the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.list_adrci_problems`.

By default, the function lists the 50 most recent problems.

This function uses the common parameter `problem_id`. For more information, see [Common parameters for diagnostic procedures \(p. 1591\)](#).

To get the task ID for all problems, call the `rdsadmin.rdsadmin_adrci_util.list_adrci_problems` function without any arguments, and store the output in a SQL client variable.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems;  
PL/SQL procedure successfully completed.
```

To read the log file, call the `rdsadmin.rds_file_util.read_text_file` function, supplying the task ID as part of the file name. In the following output, the log file shows three problems: 1, 2, and 3.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',  
'dbtask-'||:task_id||'.log'));  
  
TEXT
```

```

2020-05-29 21:18:50.764 UTC [INFO ] Listing ADRCI problems.
2020-05-29 21:18:50.829 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*****
PROBLEM_ID   PROBLEM_KEY                               LAST INCIDENT
LASTINC_TIME
-----
2          ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_003 53523
2020-05-29 20:15:20.928000 +00:00
3          ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_002 53522
2020-05-29 20:15:15.247000 +00:00
1          ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_001 53521
2020-05-29 20:15:06.047000 +00:00
3 rows fetched

2020-05-29 21:18:50.829 UTC [INFO ] The ADRCI problems were successfully listed.
2020-05-29 21:18:50.829 UTC [INFO ] The task finished successfully.

14 rows selected.

```

In the following example, you list problem 3 only.

```

SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems(problem_id=>3);
PL/SQL procedure successfully completed.

```

To read the log file for problem 3, call `rdsadmin.rds_file_util.read_text_file`. Supply the task ID as part of the file name.

```

SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
'dbtask-'||:task_id||'.log'));
TEXT
-----
2020-05-29 21:19:42.533 UTC [INFO ] Listing ADRCI problems.
2020-05-29 21:19:42.599 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*****
PROBLEM_ID   PROBLEM_KEY                               LAST INCIDENT
LASTINC_TIME
-----
3          ORA 700 [EVENT_CREATED INCIDENT] [942] [SIMULATED_ERROR_002 53522
2020-05-29 20:15:15.247000 +00:00
1 rows fetched

2020-05-29 21:19:42.599 UTC [INFO ] The ADRCI problems were successfully listed.
2020-05-29 21:19:42.599 UTC [INFO ] The task finished successfully.

12 rows selected.

```

Creating incident packages

You can create incident packages using the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.create_adrci_package`. The output is a .zip file that you can supply to Oracle Support.

This function uses the following common parameters:

- problem_id
- incident_id

Make sure to specify one of the preceding parameters. If you specify both parameters, incident_id overrides problem_id. For more information, see [Common parameters for diagnostic procedures \(p. 1591\)](#).

To create a package for a specific incident, call the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.create_adrci_package` with the incident_id parameter. The following example creates a package for incident 53523.

```
SQL> EXEC :task_id :=  
rdsadmin.rdsadmin_adrci_util.create_adrci_package(incident_id=>53523);  
  
PL/SQL procedure successfully completed.
```

To read the log file, call the `rdsadmin.rds_file_util.read_text_file`. You can supply the task ID as part of the file name. The output shows that you generated incident package ORA700EVE_20200529212043_COM_1.zip.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',  
'dbtask-'||:task_id||'.log'));  
  
TEXT  
-----  
2020-05-29 21:20:43.031 UTC [INFO ] The ADRCI package is being created.  
2020-05-29 21:20:47.641 UTC [INFO ] Generated package 1 in file /rdsdbdata/log/trace/  
ORA700EVE_20200529212043_COM_1.zip, mode complete  
2020-05-29 21:20:47.642 UTC [INFO ] The ADRCI package was successfully created.  
2020-05-29 21:20:47.642 UTC [INFO ] The task finished successfully.
```

To package diagnostic data for a particular problem, specify its ID using the problem_id parameter. In the following example, you package data for problem 3 only.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.create_adrci_package(problem_id=>3);  
  
PL/SQL procedure successfully completed.
```

To read the task output, call `rdsadmin.rds_file_util.read_text_file`, supplying the task ID as part of the file name. The output shows that you generated incident package ORA700EVE_20200529212111_COM_1.zip.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',  
'dbtask-'||:task_id||'.log'));  
  
TEXT  
-----  
2020-05-29 21:21:11.050 UTC [INFO ] The ADRCI package is being created.  
2020-05-29 21:21:15.646 UTC [INFO ] Generated package 2 in file /rdsdbdata/log/trace/  
ORA700EVE_20200529212111_COM_1.zip, mode complete  
2020-05-29 21:21:15.646 UTC [INFO ] The ADRCI package was successfully created.  
2020-05-29 21:21:15.646 UTC [INFO ] The task finished successfully.
```

Showing trace files

You can show trace files using the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile`.

This function uses the following parameter.

Parameter name	Data type	Valid values	Default	Required	Description
filename	varchar2	A valid trace file name	Null	No	If the value is null, the function shows all trace files. If it isn't null, the function shows the specified file.

To show the trace file, call the Amazon RDS function `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile` with the `incident_id` parameter.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile;
PL/SQL procedure successfully completed.
```

To list the trace file names, call the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`, supplying the task ID as part of the file name.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
'dbtask-'||:task_id||'.log')) WHERE TEXT LIKE '%/alert_%';
TEXT
-----
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-28
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-27
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-26
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-25
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-24
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-23
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-22
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-21
diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log

9 rows selected.
```

In the following example, you generate output for `alert_ORCL.log`.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile('diag/rdbms/orcl_a/
ORCL/trace/alert_ORCL.log');

PL/SQL procedure successfully completed.
```

To read the log file, call `rdsadmin.rds_file_util.read_text_file`. Supply the task ID as part of the file name. The output shows the first 10 lines of `alert_ORCL.log`.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
'dbtask-'||:task_id||'.log')) WHERE ROWNUM <= 10;
TEXT
-----
2020-05-29 21:24:02.083 UTC [INFO ] The trace files are being displayed.
2020-05-29 21:24:02.128 UTC [INFO ] Thu May 28 23:59:10 2020
Thread 1 advanced to log sequence 2048 (LGWR switch)
Current log# 3 seq# 2048 mem# 0: /rdsdbdata/db/ORCL_A/onlinelog/o1_mf_3_hbl2p8xs_.log
```

```
Thu May 28 23:59:10 2020
Archived Log entry 2037 added for thread 1 sequence 2047 ID 0x5d62ce43 dest 1:
Fri May 29 00:04:10 2020
Thread 1 advanced to log sequence 2049 (LGWR switch)
  Current log# 4 seq# 2049 mem# 0: /rdsdbdata/db/ORCL_A/onlinelog/o1_mf_4_hb12qgmh_.log
Fri May 29 00:04:10 2020

10 rows selected.
```

Performing miscellaneous tasks for Oracle DB instances

Following, you can find how to perform miscellaneous DBA tasks on your Amazon RDS DB instances running Oracle. To deliver a managed service experience, Amazon RDS doesn't provide shell access to DB instances, and restricts access to certain system procedures and tables that require advanced privileges.

Topics

- [Creating and dropping directories in the main data storage space \(p. 1597\)](#)
- [Listing files in a DB instance directory \(p. 1598\)](#)
- [Reading files in a DB instance directory \(p. 1598\)](#)
- [Accessing Opatch files \(p. 1599\)](#)
- [Managing advisor tasks \(p. 1601\)](#)

Creating and dropping directories in the main data storage space

To create directories, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.create_directory`. You can create up to 10,000 directories, all located in your main data storage space. To drop directories, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.drop_directory`.

The `create_directory` and `drop_directory` procedures have the following required parameter.

Parameter name	Data type	Default	Required	Description
<code>p_directory_name</code>	varchar2	—	Yes	The name of the directory.

The following example creates a new directory named `PRODUCT_DESCRIPTIONS`.

```
EXEC rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'product_descriptions');
```

The data dictionary stores the directory name in uppercase. You can list the directories by querying `DBA_DIRECTORIES`. The system chooses the actual host pathname automatically. The following example gets the directory path for the directory named `PRODUCT_DESCRIPTIONS`:

```
SELECT DIRECTORY_PATH
  FROM DBA_DIRECTORIES
 WHERE DIRECTORY_NAME='PRODUCT_DESCRIPTIONS';

DIRECTORY_PATH
-----
```

```
/rdsdbdata/userdirs/01
```

The master user name for the DB instance has read and write privileges in the new directory, and can grant access to other users. EXECUTE privileges are not available for directories on a DB instance. Directories are created in your main data storage space and will consume space and I/O bandwidth.

The following example drops the directory named PRODUCT_DESCRIPTIONS.

```
EXEC rdsadmin.rdsadmin_util.drop_directory(p_directory_name => 'product_descriptions');
```

Note

You can also drop a directory by using the Oracle SQL command `DROP DIRECTORY`.

Dropping a directory doesn't remove its contents. Because the `rdsadmin.rdsadmin_util.create_directory` procedure can reuse pathnames, files in dropped directories can appear in a newly created directory. Before you drop a directory, we recommend that you use `UTL_FILE.FREMOVE` to remove files from the directory. For more information, see [FREMOVE procedure](#) in the Oracle documentation.

Listing files in a DB instance directory

To list the files in a directory, use the Amazon RDS procedure `rdsadmin.rds_file_util.listdir`. The `listdir` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_directory	varchar2	—	Yes	The name of the directory to list.

The following example grants read/write privileges on the directory PRODUCT_DESCRIPTIONS to user `rdsadmin`, and then lists the files in this directory.

```
GRANT READ,WRITE ON DIRECTORY PRODUCT_DESCRIPTIONS TO rdsadmin;
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'PRODUCT_DESCRIPTIONS'));
```

Reading files in a DB instance directory

To read a text file, use the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`. The `read_text_file` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_directory	varchar2	—	Yes	The name of the directory that contains the file.
p_filename	varchar2	—	Yes	The name of the file to read.

The following example creates the file `rice.txt` in the directory PRODUCT_DESCRIPTIONS.

```
declare
  fh sys.util_file.file_type;
```

```
begin
    fh := utl_file.fopen(location=>'PRODUCT_DESCRIPTIONS', filename=>'rice.txt',
open_mode=>'w');
    utl_file.put(file=>fh, buffer=>'AnyCompany brown rice, 15 lbs');
    utl_file.fclose(file=>fh);
end;
/
```

The following example reads the file `rice.txt` from the directory `PRODUCT_DESCRIPTIONS`.

```
SELECT * FROM TABLE
  (rdsadmin.rds_file_util.read_text_file(
    p_directory => 'PRODUCT_DESCRIPTIONS',
    p_filename  => 'rice.txt'));
```

Accessing Opatch files

Opatch is an Oracle utility that enables the application and rollback of patches to Oracle software. The Oracle mechanism for determining which patches have been applied to a database is the `opatch lsinventory` command. To open service requests for Bring Your Own Licence (BYOL) customers, Oracle Support requests the `lsinventory` file and sometimes the `lsinventory_detail` file generated by Opatch.

To deliver a managed service experience, Amazon RDS doesn't provide shell access to Opatch. Instead, the `lsinventory-dbv.txt` in the `BDUMP` directory contains the patch information related to your current engine version. When you perform a minor or major upgrade, Amazon RDS updates `lsinventory-dbv.txt` within an hour of applying the patch. To verify the applied patches, read `lsinventory-dbv.txt`. This action is similar to running the `opatch lsinventory` command.

Note

The examples in this section assume that the `BDUMP` directory is named `BDUMP`. On a read replica, the `BDUMP` directory name is different. To learn how to get the `BDUMP` name by querying `V$DATABASE.DB_UNIQUE_NAME` on a read replica, see [Listing files \(p. 710\)](#).

The inventory files use the Amazon RDS naming convention `lsinventory-dbv.txt` and `lsinventory_detail-dbv.txt`, where `dbv` is the full name of your DB version. The `lsinventory-dbv.txt` file is available on all DB versions. The corresponding `lsinventory_detail-dbv.txt` is available on the following DB versions:

- 19.0.0.0, ru-2020-01.rur-2020-01.r1 or later
- 12.2.0.1, ru-2020-01.rur-2020-01.r1 or later
- 12.1.0.2, v19 or later

For example, if your DB version is `19.0.0.0.ru-2021-07.rur-2021-07.r1`, then your inventory files have the following names.

```
lsinventory-19.0.0.0.ru-2021-07.rur-2021-07.r1.txt
lsinventory_detail-19.0.0.0.ru-2021-07.rur-2021-07.r1.txt
```

Ensure that you download the files that match the current version of your DB engine.

Console

To download an inventory file using the console

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that has the log file that you want to view.
4. Choose the **Logs & events** tab.
5. Scroll down to the **Logs** section.
6. In the **Logs** section, search for `lsinventory`.
7. Select the file that you want to access, and then choose **Download**.

SQL

To read the `lsinventory-dbv.txt` in a SQL client, you can use a `SELECT` statement. For this technique, use either of the following `rdsadmin` functions: `rdsadmin.rds_file_util.read_text_file` or `rdsadmin.tracefile_listing`.

In the following sample query, replace `dbv` with your Oracle DB version. For example, your DB version might be `19.0.0.0.ru-2020-04.rur-2020-04.r1`.

```
SELECT text
FROM   TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP', 'lsinventory-dbv.txt'));
```

PL/SQL

To read the `lsinventory-dbv.txt` in a SQL client, you can write a PL/SQL program. This program uses `utl_file` to read the file, and `dbms_output` to print it. These are Oracle-supplied packages.

In the following sample program, replace `dbv` with your Oracle DB version. For example, your DB version might be `19.0.0.0.ru-2020-04.rur-2020-04.r1`.

```
SET SERVEROUTPUT ON
DECLARE
  v_file          SYS.UTL_FILE.FILE_TYPE;
  v_line          VARCHAR2(1000);
  v_oracle_home_type  VARCHAR2(1000);
  c_directory    VARCHAR2(30) := 'BDUMP';
  c_output_file   VARCHAR2(30) := 'lsinventory-dbv.txt';
BEGIN
  v_file := SYS.UTL_FILE.FOPEN(c_directory, c_output_file, 'r');
  LOOP
    BEGIN
      SYS.UTL_FILE.GET_LINE(v_file, v_line,1000);
      DBMS_OUTPUT.PUT_LINE(v_line);
    EXCEPTION
      WHEN no_data_found THEN
        EXIT;
    END;
  END LOOP;
END;
/
```

Or query `rdsadmin.tracefile_listing`, and spool the output to a file. The following example spools the output to `/tmp/tracefile.txt`.

```
SPPOOL /tmp/tracefile.txt
SELECT *
FROM   rdsadmin.tracefile_listing
WHERE  FILENAME LIKE 'lsinventory%';
SPOOL OFF;
```

Managing advisor tasks

Oracle Database includes a number of advisors. Each advisor supports automated and manual tasks. You can use procedures in the `rdsadmin.rdsadmin_util` package to manage some advisor tasks.

The advisor task procedures are available in the following engine versions:

- Oracle Database 21c (21.0.0)
- Version 19.0.0.0.ru-2021-01.rur-2021-01.r1 and higher Oracle Database 19c versions

For more information, see [Version 19.0.0.0.ru-2021-01.rur-2021-01.r1](#) in the *Amazon RDS for Oracle Release Notes*.

- Version 12.2.0.1.ru-2021-01.rur-2021-01.r1 and higher Oracle Database 12c (Release 2) 12.2.0.1 versions

For more information, see [Version 12.2.0.1.ru-2021-01.rur-2021-01.r1](#) in the *Amazon RDS for Oracle Release Notes*.

Topics

- [Setting parameters for advisor tasks \(p. 1601\)](#)
- [Disabling AUTO_STATS_ADVISOR_TASK \(p. 1602\)](#)
- [Re-enabling AUTO_STATS_ADVISOR_TASK \(p. 1603\)](#)

Setting parameters for advisor tasks

To set parameters for some advisor tasks, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.advisor_task_set_parameter`. The `advisor_task_set_parameter` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
<code>p_task_name</code>	<code>varchar2</code>	—	Yes	<p>The name of the advisor task whose parameters you want to change. The following values are valid:</p> <ul style="list-style-type: none">• <code>AUTO_STATS_ADVISOR_TASK</code>• <code>INDIVIDUAL_STATS_ADVISOR_TASK</code>• <code>SYS_AUTO_SPM_EVOLVE_TASK</code>• <code>SYS_AUTO_SQL_TUNING_TASK</code>
<code>p_parameter</code>	<code>varchar2</code>	—	Yes	<p>The name of the task parameter. To find valid parameters for an advisor task, run the following query. Substitute <code>p_task_name</code> with a valid value for <code>p_task_name</code>:</p> <pre>COL PARAMETER_NAME FORMAT a30 COL PARAMETER_VALUE FORMAT a30 SELECT PARAMETER_NAME, PARAMETER_VALUE FROM DBA_ADVISOR_PARAMETERS WHERE TASK_NAME='p_task_name' AND PARAMETER_VALUE != 'UNUSED' ORDER BY PARAMETER_NAME;</pre>

Parameter name	Data type	Default	Required	Description
p_value	varchar2	—	Yes	<p>The value for a task parameter. To find valid values for task parameters, run the following query. Substitute <i>p_task_name</i> with a valid value for p_task_name:</p> <pre>COL PARAMETER_NAME FORMAT a30 COL PARAMETER_VALUE FORMAT a30 SELECT PARAMETER_NAME, PARAMETER_VALUE FROM DBA_ADVISOR_PARAMETERS WHERE TASK_NAME='<i>p_task_name</i>' AND PARAMETER_VALUE != 'UNUSED' ORDER BY PARAMETER_NAME;</pre>

The following PL/SQL program sets ACCEPT_PLANS to FALSE for SYS_AUTO_SPM_EVOLVE_TASK. The SQL Plan Management automated task verifies the plans and generates a report of its findings, but does not evolve the plans automatically. You can use a report to identify new SQL plan baselines and accept them manually.

```
BEGIN
  rdsadmin.rdsadmin_util.advisor_task_set_parameter(
    p_task_name => 'SYS_AUTO_SPM_EVOLVE_TASK',
    p_parameter => 'ACCEPT_PLANS',
    p_value      => 'FALSE');
END;
```

The following PL/SQL program sets EXECUTION_DAYS_TO_EXPIRE to 10 for AUTO_STATS_ADVISOR_TASK. The predefined task AUTO_STATS_ADVISOR_TASK runs automatically in the maintenance window once per day. The example sets the retention period for the task execution to 10 days.

```
BEGIN
  rdsadmin.rdsadmin_util.advisor_task_set_parameter(
    p_task_name => 'AUTO_STATS_ADVISOR_TASK',
    p_parameter => 'EXECUTION_DAYS_TO_EXPIRE',
    p_value      => '10');
END;
```

Disabling AUTO_STATS_ADVISOR_TASK

To disable AUTO_STATS_ADVISOR_TASK, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.advisor_task_drop`. The `advisor_task_drop` procedure accepts the following parameter.

Note

This procedure is available in Oracle Database 12c Release 2 (12.2.0.1) and later.

Parameter name	Data type	Default	Required	Description
p_task_name	varchar2	—	Yes	The name of the advisor task to be disabled. The only valid value is AUTO_STATS_ADVISOR_TASK.

The following command drops AUTO_STATS_ADVISOR_TASK.

```
EXEC rdsadmin.rdsadmin_util.advisor_task_drop('AUTO_STATS_ADVISOR_TASK')
```

You can re-enabling AUTO_STATS_ADVISOR_TASK using
`rdsadmin.rdsadmin_util.dbms_stats_init`.

Re-enabling AUTO_STATS_ADVISOR_TASK

To re-enable AUTO_STATS_ADVISOR_TASK, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.dbms_stats_init`. The `dbms_stats_init` procedure takes no parameters.

The following command re-enables AUTO_STATS_ADVISOR_TASK.

```
EXEC rdsadmin.rdsadmin_util.dbms_stats_init()
```

Configuring advanced RDS for Oracle features

RDS for Oracle supports various advanced features, including HugePages, an instance store, and extended data types.

Topics

- [Storing temporary data in an RDS for Oracle instance store \(p. 1604\)](#)
- [Turning on HugePages for an RDS for Oracle instance \(p. 1610\)](#)
- [Turning on extended data types in RDS for Oracle \(p. 1613\)](#)

Storing temporary data in an RDS for Oracle instance store

Use an instance store for the temporary tablespaces and the Database Smart Flash Cache (the flash cache) on supported RDS for Oracle DB instance classes.

Topics

- [Overview of the RDS for Oracle instance store \(p. 1604\)](#)
- [Turning on an RDS for Oracle instance store \(p. 1606\)](#)
- [Configuring an RDS for Oracle instance store \(p. 1606\)](#)
- [Considerations when changing the DB instance type \(p. 1608\)](#)
- [Working with an instance store on an Oracle read replica \(p. 1609\)](#)
- [Configuring a temporary tablespace group on an instance store and Amazon EBS \(p. 1609\)](#)
- [Removing an RDS for Oracle instance store \(p. 1610\)](#)

Overview of the RDS for Oracle instance store

An *instance store* provides temporary block-level storage for an RDS for Oracle DB instance. You can use an instance store for temporary storage of information that changes frequently.

An instance store is based on Non-Volatile Memory Express (NVMe) devices that are physically attached to the host computer. The storage is optimized for low latency, random I/O performance, and sequential read throughput.

The size of the instance store varies by DB instance type. For more information about the instance store, see [Amazon EC2 instance store](#) in the *Amazon Elastic Compute Cloud User Guide for Linux Instances*.

Topics

- [Types of data in the RDS for Oracle instance store \(p. 1604\)](#)
- [Benefits of the RDS for Oracle instance store \(p. 1605\)](#)
- [Supported instance classes for the RDS for Oracle instance store \(p. 1605\)](#)
- [Supported engine versions for the RDS for Oracle instance store \(p. 1606\)](#)
- [Supported AWS Regions for the RDS for Oracle instance store \(p. 1606\)](#)
- [Cost of the RDS for Oracle instance store \(p. 1606\)](#)

Types of data in the RDS for Oracle instance store

You can place the following types of RDS for Oracle temporary data in an instance store:

A temporary tablespace

Oracle Database uses temporary tablespaces to store intermediate query results that don't fit in memory. Larger queries can generate large amounts of intermediate data that needs to be cached temporarily, but doesn't need to persist. In particular, a temporary tablespace is useful for sorts, hash aggregations, and joins. If your RDS for Oracle DB instance uses the Enterprise Edition or Standard Edition 2, you can place a temporary tablespace in an instance store.

The flash cache

The flash cache improves the performance of single-block random reads in the conventional path. A best practice is to size the cache to accommodate most of your active data set. If your RDS for Oracle DB instance uses the Enterprise Edition, you can place the flash cache in an instance store.

By default, an instance store is configured for a temporary tablespace but not for the flash cache. You can't place Oracle data files and database log files in an instance store.

Benefits of the RDS for Oracle instance store

You might consider using an instance store to store temporary files and caches that you can afford to lose. If you want to improve DB performance, or if an increasing workload is causing performance problems for your Amazon EBS storage, consider scaling to an instance class that supports an instance store.

By placing your temporary tablespace and flash cache on an instance store, you get the following benefits:

- Lower read latencies
- Higher throughput
- Reduced load on your Amazon EBS volumes
- Lower storage and snapshot costs because of reduced Amazon EBS load
- Less need to provision high IOPS, possibly lowering your overall cost

By placing your temporary tablespace on the instance store, you deliver an immediate performance boost to queries that use temporary space. When you place the flash cache on the instance store, cached block reads typically have much lower latency than Amazon EBS reads. The flash cache needs to be "warmed up" before it delivers performance benefits. The cache warms up by itself because the database writes blocks to the flash cache as they age out of the database buffer cache.

Note

In some cases, the flash cache causes performance overhead because of cache management. Before you turn on the flash cache in a production environment, we recommend that you analyze your workload and test the cache in a test environment.

Supported instance classes for the RDS for Oracle instance store

Amazon RDS supports the instance store for the following instance classes:

- db.m5d
- db.r5d

RDS for Oracle supports the preceding instance classes for the BYOL licensing model only. For more information, see [Supported RDS for Oracle instance classes \(p. 1477\)](#) and [Bring Your Own License \(BYOL\) \(p. 1474\)](#).

To see the total instance storage for the supported instance types, run the following command in the AWS CLI.

Example

```
aws ec2 describe-instance-types \
--filters "Name=instance-type,Values=*5d.*large*" \
--query "[InstanceTypes[?contains(InstanceType,'m5d')||contains(InstanceType,'r5d')]] \
[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
--output table
```

The preceding command returns the raw device size for the instance store. RDS for Oracle uses a small portion of this space for configuration. The space in the instance store that is available for temporary tablespaces or the flash cache is slightly smaller.

Supported engine versions for the RDS for Oracle instance store

The instance store is supported for the following RDS for Oracle engine versions:

- 21.0.0.0.ru-2022-01.rur-2022-01.r1 or higher Oracle Database 21c versions
- 19.0.0.0.ru-2021-10.rur-2021-10.r1 or higher Oracle Database 19c versions

Supported AWS Regions for the RDS for Oracle instance store

The instance store is available in all AWS Regions where one or more of these instance types are supported. For more information on the db.m5d and db.r5d instance classes, see [DB instance classes \(p. 10\)](#). For more information on the instance classes supported by Amazon RDS for Oracle, see [RDS for Oracle instance classes \(p. 1477\)](#).

Cost of the RDS for Oracle instance store

The cost of the instance store is built into the cost of the instance-store turned on instances. You don't incur additional costs by enabling an instance store on an RDS for Oracle DB instance. For more information about instance-store turned on instances, see [Supported instance classes for the RDS for Oracle instance store \(p. 1605\)](#).

Turning on an RDS for Oracle instance store

To turn on the instance store for RDS for Oracle temporary data, do one of the following:

- Create an RDS for Oracle DB instance using a supported instance class. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- Modify an existing RDS for Oracle DB instance to use a supported instance class. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Configuring an RDS for Oracle instance store

By default, 100% of instance store space is allocated to the temporary tablespace. To configure the instance store to allocate space to the flash cache and temporary tablespace, set the following parameters in the parameter group for your instance:

db_flash_cache_size={DBInstanceStore*{0,2,4,6,8,10}/10}

This parameter specifies the amount of storage space allocated for the flash cache. This parameter is valid only for Oracle Database Enterprise Edition. The default value is $\{DBInstanceStore*0/10\}$. If you set a nonzero value for `db_flash_cache_size`, your RDS for Oracle instance enables the flash cache after you restart the instance.

rds.instance_store_temp_size={DBInstanceStore*{0,2,4,6,8,10}/10}

This parameter specifies the amount of storage space allocated for the temporary tablespace. The default value is $\{DBInstanceStore*10/10\}$. This parameter is modifiable for Oracle Database Enterprise Edition and read-only for Standard Edition 2. If you set a nonzero value for `rds.instance_store_temp_size`, Amazon RDS allocates space in the instance store for the temporary tablespace.

You can set the `db_flash_cache_size` and `rds.instance_store_temp_size` parameters for DB instances that don't use an instance store. In this case, both settings evaluate to 0 , which turns off the feature. In this case, you can use the same parameter group for different instance sizes and for instances that don't use an instance store. If you modify these parameters, make sure to reboot the associated instances so that the changes can take effect.

Important

If you allocate space for a temporary tablespace, Amazon RDS doesn't create the temporary tablespace automatically. To learn how to create the temporary tablespace on the instance store, see [Creating a temporary tablespace on the instance store \(p. 1545\)](#).

The combined value of the preceding parameters must not exceed 10/10, or 100%. The following table illustrates valid and invalid parameter settings.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explanation
<code>db_flash_cache_size={DBInstanceStore*0/10}</code>	<code>instance_store_temp_size={DBInstanceStore*10/10}</code>	This is a valid configuration for all editions of Oracle Database. Amazon RDS allocates 100% of instance store space to the temporary tablespace. This is the default.
<code>db_flash_cache_size={DBInstanceStore*10/10}</code>	<code>instance_store_temp_size={DBInstanceStore*0/10}</code>	This is a valid configuration for Oracle Database Enterprise Edition only. Amazon RDS allocates 100% of instance store space to the flash cache.
<code>db_flash_cache_size={DBInstanceStore*2/10}</code>	<code>instance_store_temp_size={DBInstanceStore*8/10}</code>	This is a valid configuration for Oracle Database Enterprise Edition only. Amazon RDS allocates 20% of instance store space to the flash cache, and 80% of instance store space to the temporary tablespace.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explanation
db_flash_cache_size={DBInstanceStore*6/10}	instance_store_temp_size={DBInstanceStore*4/10}	This is a valid configuration for Oracle Database Enterprise Edition only. Amazon RDS allocates 60% of instance store space to the flash cache, and 40% of instance store space to the temporary tablespace.
db_flash_cache_size={DBInstanceStore*2/10}	instance_store_temp_size={DBInstanceStore*4/10}	This is a valid configuration for Oracle Database Enterprise Edition only. Amazon RDS allocates 20% of instance store space to the flash cache, and 40% of instance store space to the temporary tablespace.
db_flash_cache_size={DBInstanceStore*8/10}	instance_store_temp_size={DBInstanceStore*8/10}	This is an invalid configuration because the combined percentage of instance store space exceeds 100%. In such cases, Amazon RDS fails the attempt.

Considerations when changing the DB instance type

If you change your DB instance type, it can affect the configuration of the flash cache or the temporary tablespace on the instance store. Consider the following modifications and their effects:

You scale up or scale down the DB instance that supports the instance store.

The following values increase or decrease proportionally to the new size of the instance store:

- The new size of the flash cache.
- The space allocated to the temporary tablespaces that reside in the instance store.

For example, the setting db_flash_cache_size={DBInstanceStore*6/10} on a db.m5d.4xlarge instance provides around 340 GB of flash cache space. If you scale up the instance type to db.m5d.8xlarge, the flash cache space increases to around 680 GB.

You modify a DB instance that doesn't use an instance store to an instance that does use an instance store.

If `db_flash_cache_size` is set to a value larger than `0`, the flash cache is configured. If `rds.instance_store_temp_size` is set to a value larger than `0`, the instance store space is allocated for use by a temporary tablespace. RDS for Oracle doesn't move tempfiles to the instance store automatically. For information about using the allocated space, see [Creating a temporary tablespace on the instance store \(p. 1545\)](#) or [Adding a tempfile to the instance store on a read replica \(p. 1545\)](#).

You modify a DB instance that uses an instance store to an instance that doesn't use an instance store.

In this case, RDS for Oracle removes the flash cache. RDS re-creates the tempfile that is currently located on the instance store on an Amazon EBS volume. The maximum size of the new tempfile is the former size of the `rds.instance_store_temp_size` parameter.

Working with an instance store on an Oracle read replica

Read replicas support the flash cache and temporary tablespaces on an instance store. While the flash cache works the same way as on the primary DB instance, note the following differences for temporary tablespaces:

- You can't create a temporary tablespace on a read replica. If you create a new temporary tablespace on the primary instance, RDS for Oracle replicates the tablespace information without tempfiles. To add a new tempfile, use either of the following techniques:
 - Use the Amazon RDS procedure `rdsadmin.rdsadmin_util.add_inst_store_tempfile`. RDS for Oracle creates a tempfile in the instance store on your read replica, and adds it to the specified temporary tablespace.
 - Run the `ALTER TABLESPACE ... ADD TEMPFILE` command. RDS for Oracle places the tempfile on Amazon EBS storage.

Note

The tempfile sizes and storage types can be different on the primary DB instance and the read replica.

- You can manage the default temporary tablespace setting only on the primary DB instance. RDS for Oracle replicates the setting to all read replicas.
- You can configure the temporary tablespace groups only on the primary DB instance. RDS for Oracle replicates the setting to all read replicas.

Configuring a temporary tablespace group on an instance store and Amazon EBS

You can configure a temporary tablespace group to include temporary tablespaces on both an instance store and Amazon EBS. This technique is useful when you want more temporary storage than is allowed by the maximum setting of `rds.instance_store_temp_size`.

When you configure a temporary tablespace group on both an instance store and Amazon EBS, the two tablespaces have significantly different performance characteristics. Oracle Database chooses the tablespace to serve queries based on an internal algorithm. Therefore, similar queries can vary in performance.

Typically, you create a temporary tablespace in the instance store as follows:

1. Create a temporary tablespace in the instance store.
2. Set the new tablespace as the database default temporary tablespace.

If the tablespace size in the instance store is insufficient, you can create additional temporary storage as follows:

1. Assign the temporary tablespace in the instance store to a temporary tablespace group.
2. Create a new temporary tablespace in Amazon EBS if one doesn't exist.
3. Assign the temporary tablespace in Amazon EBS to the same tablespace group that includes the instance store tablespace.
4. Set the tablespace group as the default temporary tablespace.

The following example assumes that the size of the temporary tablespace in the instance store doesn't meet your application requirements. The example creates the temporary tablespace `temp_in_inst_store` in the instance store, assigns it to tablespace group `temp_group`, adds the existing Amazon EBS tablespace named `temp_in_ebs` to this group, and sets this group as the default temporary tablespace.

```
SQL> EXEC rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace('temp_in_inst_store');

PL/SQL procedure successfully completed.

SQL> ALTER TABLESPACE temp_in_inst_store TABLESPACE GROUP temp_group;

Tablespace altered.

SQL> ALTER TABLESPACE temp_in_ebs TABLESPACE GROUP temp_group;

Tablespace altered.

SQL> EXEC rdsadmin.rdsadmin_util.alter_default_temp_tablespace('temp_group');

PL/SQL procedure successfully completed.

SQL> SELECT * FROM DBA_TABLESPACE_GROUPS;

GROUP_NAME          TABLESPACE_NAME
-----
TEMP_GROUP          TEMP_IN_EBS
TEMP_GROUP          TEMP_IN_INST_STORE

SQL> SELECT PROPERTY_VALUE FROM DATABASE_PROPERTIES WHERE
PROPERTY_NAME='DEFAULT_TEMP_TABLESPACE';

PROPERTY_VALUE
-----
TEMP_GROUP
```

Removing an RDS for Oracle instance store

To remove the instance store, modify your RDS for Oracle DB instance to use an instance type that doesn't support instance store, such as db.m5 or db.r5.

Turning on HugePages for an RDS for Oracle instance

Amazon RDS for Oracle supports Linux kernel HugePages for increased database scalability. HugePages results in smaller page tables and less CPU time spent on memory management, increasing the performance of large database instances. For more information, see [Overview of HugePages](#) in the Oracle documentation.

You can use HugePages with all supported versions and editions of RDS for Oracle.

The `use_large_pages` parameter controls whether HugePages are turned on for a DB instance. The possible settings for this parameter are `ONLY`, `FALSE`, and `{DBInstanceClassHugePagesDefault}`. The `use_large_pages` parameter is set to `{DBInstanceClassHugePagesDefault}` in the default DB parameter group for Oracle.

To control whether HugePages are turned on for a DB instance automatically, you can use the `DBInstanceClassHugePagesDefault` formula variable in parameter groups. The value is determined as follows:

- For the DB instance classes mentioned in the table following, `DBInstanceClassHugePagesDefault` always evaluates to `FALSE` by default, and `use_large_pages` evaluates to `FALSE`. You can turn on HugePages manually for these DB instance classes if the DB instance class has at least 14 GiB of memory.
- For DB instance classes not mentioned in the table following, if the DB instance class has less than 14 GiB of memory, `DBInstanceClassHugePagesDefault` always evaluates to `FALSE`. Also, `use_large_pages` evaluates to `FALSE`.
- For DB instance classes not mentioned in the table following, if the instance class has at least 14 GiB of memory and less than 100 GiB of memory, `DBInstanceClassHugePagesDefault` evaluates to `TRUE` by default. Also, `use_large_pages` evaluates to `ONLY`. You can turn off HugePages manually by setting `use_large_pages` to `FALSE`.
- For DB instance classes not mentioned in the table following, if the instance class has at least 100 GiB of memory, `DBInstanceClassHugePagesDefault` always evaluates to `TRUE`. Also, `use_large_pages` evaluates to `ONLY` and HugePages can't be disabled.

HugePages are not turned on by default for the following DB instance classes.

DB instance class family	DB instance classes with HugePages not turned on by default
db.m5	db.m5.large
db.m4	db.m4.large, db.m4.xlarge, db.m4.2xlarge, db.m4.4xlarge, db.m4.10xlarge
db.t3	db.t3.micro, db.t3.small, db.t3.medium, db.t3.large

For more information about DB instance classes, see [Hardware specifications for DB instance classes \(p. 55\)](#).

To turn on HugePages for new or existing DB instances manually, set the `use_large_pages` parameter to `ONLY`. You can't use HugePages with Oracle Automatic Memory Management (AMM). If you set the parameter `use_large_pages` to `ONLY`, then you must also set both `memory_target` and `memory_max_target` to `0`. For more information about setting DB parameters for your DB instance, see [Working with parameter groups \(p. 289\)](#).

You can also set the `sga_target`, `sga_max_size`, and `pga_aggregate_target` parameters. When you set system global area (SGA) and program global area (PGA) memory parameters, add the values together. Subtract this total from your available instance memory (`DBInstanceClassMemory`) to determine the free memory beyond the HugePages allocation. You must leave free memory of at least 2 GiB, or 10 percent of the total available instance memory, whichever is smaller.

After you configure your parameters, you must reboot your DB instance for the changes to take effect. For more information, see [Rebooting a DB instance \(p. 366\)](#).

Note

The Oracle DB instance defers changes to SGA-related initialization parameters until you reboot the instance without failover. In the Amazon RDS console, choose **Reboot** but *do not* choose

Reboot with failover. In the AWS CLI, call the `reboot-db-instance` command with the `--no-force-failover` parameter. The DB instance does not process the SGA-related parameters during failover or during other maintenance operations that cause the instance to restart.

The following is a sample parameter configuration for HugePages that enables HugePages manually. You should set the values to meet your needs.

```
memory_target          = 0
memory_max_target     = 0
pga_aggregate_target = {DBInstanceClassMemory*1/8}
sga_target            = {DBInstanceClassMemory*3/4}
sga_max_size          = {DBInstanceClassMemory*3/4}
use_large_pages       = ONLY
```

Assume the following parameters values are set in a parameter group.

```
memory_target          = IF({DBInstanceClassHugePagesDefault}, 0,
{DBInstanceClassMemory*3/4})
memory_max_target     = IF({DBInstanceClassHugePagesDefault}, 0,
{DBInstanceClassMemory*3/4})
pga_aggregate_target = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*1/8}, 0)
sga_target            = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*3/4}, 0)
sga_max_size          = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*3/4}, 0)
use_large_pages       = {DBInstanceClassHugePagesDefault}
```

The parameter group is used by a db.r4 DB instance class with less than 100 GiB of memory. With these parameter settings and `use_large_pages` set to `{DBInstanceClassHugePagesDefault}`, HugePages are turned on for the db.r4 instance.

Consider another example with following parameters values set in a parameter group.

```
memory_target          = IF({DBInstanceClassHugePagesDefault}, 0,
{DBInstanceClassMemory*3/4})
memory_max_target     = IF({DBInstanceClassHugePagesDefault}, 0,
{DBInstanceClassMemory*3/4})
pga_aggregate_target = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*1/8}, 0)
sga_target            = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*3/4}, 0)
sga_max_size          = IF({DBInstanceClassHugePagesDefault},
{DBInstanceClassMemory*3/4}, 0)
use_large_pages       = FALSE
```

The parameter group is used by a db.r4 DB instance class and a db.r5 DB instance class, both with less than 100 GiB of memory. With these parameter settings, HugePages are turned off on the db.r4 and db.r5 instance.

Note

If this parameter group is used by a db.r4 DB instance class or db.r5 DB instance class with at least 100 GiB of memory, the FALSE setting for `use_large_pages` is overridden and set to ONLY. In this case, a customer notification regarding the override is sent.

After HugePages are active on your DB instance, you can view HugePages information by enabling enhanced monitoring. For more information, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

Turning on extended data types in RDS for Oracle

Amazon RDS Oracle Database 12c supports extended data types. With extended data types, the maximum size is 32,767 bytes for the VARCHAR2, NVARCHAR2, and RAW data types. To use extended data types, set the MAX_STRING_SIZE parameter to EXTENDED. For more information, see [Extended data types](#) in the Oracle documentation.

If you don't want to use extended data types, keep the MAX_STRING_SIZE parameter set to STANDARD (the default). In this case, the size limits are 4,000 bytes for the VARCHAR2 and NVARCHAR2 data types, and 2,000 bytes for the RAW data type.

You can turn on extended data types on a new or existing DB instance. For new DB instances, DB instance creation time is typically longer when you turn on extended data types. For existing DB instances, the DB instance is unavailable during the conversion process.

The following are considerations for a DB instance with extended data types enabled:

- When you turn on extended data types for a DB instance, you can't change the DB instance back to use the standard size for data types. After a DB instance is converted to use extended data types, if you set the MAX_STRING_SIZE parameter back to STANDARD it results in the incompatible-parameters status.
- When you restore a DB instance that uses extended data types, you must specify a parameter group with the MAX_STRING_SIZE parameter set to EXTENDED. During restore, if you specify the default parameter group or any other parameter group with MAX_STRING_SIZE set to STANDARD it results in the incompatible-parameters status.
- We recommend that you don't turn on extended data types for Oracle DB instances running on the t2.micro DB instance class.

When the DB instance status is incompatible-parameters because of the MAX_STRING_SIZE setting, the DB instance remains unavailable until you set the MAX_STRING_SIZE parameter to EXTENDED and reboot the DB instance.

Turning on extended data types for a new DB instance

To turn on extended data types for a new DB instance

1. Set the MAX_STRING_SIZE parameter to EXTENDED in a parameter group.

To set the parameter, you can either create a new parameter group or modify an existing parameter group.

For more information, see [Working with parameter groups \(p. 289\)](#).

2. Create a new Amazon RDS Oracle DB instance, and associate the parameter group with MAX_STRING_SIZE set to EXTENDED with the DB instance.

For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Turning on extended data types for an existing DB instance

When you modify a DB instance to turn on extended data types, the data in the database is converted to use the extended sizes. The DB instance is unavailable during the conversion. The amount of time it takes to convert the data depends on the DB instance class used by the DB instance and the size of the database.

Note

After you turn on extended data types, you can't perform a point-in-time restore to a time during the conversion. You can restore to the time immediately before the conversion or after the conversion.

To turn on extended data types for an existing DB instance

1. Take a snapshot of the database.

If there are invalid objects in the database, Amazon RDS tries to recompile them. The conversion to extended data types can fail if Amazon RDS can't recompile an invalid object. The snapshot enables you to restore the database if there is a problem with the conversion. Always check for invalid objects before conversion and fix or drop those invalid objects. For production databases, we recommend testing the conversion process on a copy of your DB instance first.

For more information, see [Creating a DB snapshot \(p. 448\)](#).

2. Set the MAX_STRING_SIZE parameter to EXTENDED in a parameter group.

To set the parameter, you can either create a new parameter group or modify an existing parameter group.

For more information, see [Working with parameter groups \(p. 289\)](#).

3. Modify the DB instance to associate it with the parameter group with MAX_STRING_SIZE set to EXTENDED.

For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

4. Reboot the DB instance for the parameter change to take effect.

For more information, see [Rebooting a DB instance \(p. 366\)](#).

Importing data into Oracle on Amazon RDS

How you import data into an Amazon RDS for Oracle DB instance depends on the following:

- The amount of data you have
- The number of database objects in your database
- The variety of database objects in your database

For example, you can use the following tools, depending on your requirements:

- Oracle SQL Developer – Import a simple, 20 MB database.
- Oracle Data Pump – Import complex databases, or databases that are several hundred megabytes or several terabytes in size. You can use Amazon S3 in this task. For example, download Data Pump files from Amazon S3 to the DB instance. For more information, see [Amazon S3 integration \(p. 1648\)](#).
- AWS Database Migration Service (AWS DMS) – Migrate databases without downtime. For more information about AWS DMS, see [What is AWS Database Migration Service](#) and the blog post [Migrating Oracle databases with near-zero downtime using AWS DMS](#).

Important

Before you use the preceding migration techniques, we recommend that you back up your database. After you import the data, you can back up your RDS for Oracle DB instances by creating snapshots. Later, you can restore the snapshots. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

For many database engines, ongoing replication can continue until you are ready to switch over to the target database. You can use AWS DMS to migrate to RDS for Oracle from either the same database engine or a different engine. If you migrate from a different database engine, you can use the AWS Schema Conversion Tool to migrate schema objects that AWS DMS doesn't migrate.

The following video summarizes the different Oracle Database migration techniques.

The following video explains how to plan and execute a data migration.

Topics

- [Importing using Oracle SQL Developer \(p. 1615\)](#)
- [Importing using Oracle Data Pump \(p. 1616\)](#)
- [Importing using Oracle Export/Import \(p. 1626\)](#)
- [Importing using Oracle SQL*Loader \(p. 1627\)](#)
- [Migrating with Oracle materialized views \(p. 1628\)](#)

Importing using Oracle SQL Developer

For small databases, you can use Oracle SQL Developer, a graphical Java tool distributed without cost by Oracle. You can install this tool on your desktop computer (Windows, Linux, or Mac) or on one of your servers. SQL Developer provides options for migrating data between two Oracle databases, or for migrating data from other databases, such as MySQL, to an Oracle database. SQL Developer is best suited for migrating small databases. We recommend that you read the Oracle SQL Developer product documentation before you begin migrating your data.

After you install SQL Developer, you can use it to connect to your source and target databases. Use the **Database Copy** command on the Tools menu to copy your data to your Amazon RDS instance.

To download SQL Developer, go to <http://www.oracle.com/technetwork/developer-tools/sql-developer>.

Oracle also has documentation on how to migrate from other databases, including MySQL and SQL Server. For more information, see <http://www.oracle.com/technetwork/database/migration> in the Oracle documentation.

Importing using Oracle Data Pump

Oracle Data Pump is a utility that allows you to export Oracle data to a dump file and import it into another Oracle database. It is a long-term replacement for the Oracle Export/Import utilities. Oracle Data Pump is the recommended way to move large amounts of data from an Oracle database to an Amazon RDS DB instance.

The examples in this section show one way to import data into an Oracle database, but Oracle Data Pump supports other techniques. For more information, see the [Oracle Database documentation](#).

The examples in this section use the DBMS_DATAPUMP package. You can accomplish the same tasks using the Oracle Data Pump command line utilities impdp and expdp. You can install these utilities on a remote host as part of an Oracle Client installation, including Oracle Instant Client. For more information, see [How do I use Oracle Instant Client to run Data Pump Import or Export for my Amazon RDS for Oracle DB instance?](#)

Topics

- [Overview of Oracle Data Pump \(p. 1616\)](#)
- [Importing data with Oracle Data Pump and an Amazon S3 bucket \(p. 1618\)](#)
- [Importing data with Oracle Data Pump and a database link \(p. 1622\)](#)

Overview of Oracle Data Pump

Oracle Data Pump is made up of the following components:

- Command-line clients expdp and impdp
- The DBMS_DATAPUMP PL/SQL package
- The DBMS_METADATA PL/SQL package

You can use Oracle Data Pump for the following scenarios:

- Import data from an Oracle database, either on-premises or on an Amazon EC2 instance, to an RDS for Oracle DB instance.
- Import data from an RDS for Oracle DB instance to an Oracle database, either on-premises or on an Amazon EC2 instance.
- Import data between RDS for Oracle DB instances, for example, to migrate data from EC2-Classic to VPC.

To download Oracle Data Pump utilities, see [Oracle database software downloads](#) on the Oracle Technology Network website. For compatibility considerations when migrating between versions of Oracle Database, see the [Oracle Database documentation](#).

Oracle Data Pump workflow

Typically, you use Oracle Data Pump in the following stages:

1. Export your data into a dump file on the source database.

2. Upload your dump file to your destination RDS for Oracle DB instance. You can transfer using an Amazon S3 bucket or by using a database link between the two databases.
3. Import the data from your dump file into your RDS for Oracle DB instance.

Oracle Data Pump best practices

When you use Oracle Data Pump to import data into an RDS for Oracle instance, we recommend the following best practices:

- Perform imports in schema or table mode to import specific schemas and objects.
- Limit the schemas you import to those required by your application.
- Don't import in full mode or import schemas for system-maintained components.

Because RDS for Oracle doesn't allow access to SYS or SYSDBA administrative users, these actions might damage the Oracle data dictionary and affect the stability of your database.

- When loading large amounts of data, do the following:
 1. Transfer the dump file to the target RDS for Oracle DB instance.
 2. Take a DB snapshot of your instance.
 3. Test the import to verify that it succeeds.

If database components are invalidated, you can delete the DB instance and re-create it from the DB snapshot. The restored DB instance includes any dump files staged on the DB instance when you took the DB snapshot.

- Don't import dump files that were created using the Oracle Data Pump export parameters TRANSPORT_TABLESPACES, TRANSPORTTABLE, or TRANSPORT_FULL_CHECK. RDS for Oracle DB instances don't support importing these dump files.
- Don't import dump files that contain Oracle Scheduler objects in SYS, SYSTEM, RDSADMIN, RDSSEC, and RDS_DATAGUARD, and belong to the following categories:
 - Jobs
 - Programs
 - Schedules
 - Chains
 - Rules
 - Evaluation contexts
 - Rule sets

RDS for Oracle DB instances don't support importing these dump files.

- To exclude unsupported Oracle Scheduler objects, use additional directives during the Data Pump export. If you use DBMS_DATAPUMP, you can add an additional METADATA_FILTER before the DBMS_METADATA.START_JOB:

```
DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl,
    'EXCLUDE_NAME_EXPR',
    q'[IN (SELECT NAME FROM SYS.OBJ$
        WHERE TYPE# IN (66,67,74,79,59,62,46)
        AND OWNER# IN
            (SELECT USER# FROM SYS.USER$
                WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC'))
        )
    ],
    'PROCOBJ'
```

);

If you use expdp, create a parameter file that contains the exclude directive shown in the following example. Then use PARFILE=*parameter_file* with your expdp command.

```
exclude=procobj:"IN
  (SELECT NAME FROM sys.OBJ$
   WHERE TYPE# IN (66,67,74,79,59,62,46)
   AND OWNER# IN
     (SELECT USER# FROM SYS.USER$
      WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC'))
  )
)"
```

Importing data with Oracle Data Pump and an Amazon S3 bucket

The following import process uses Oracle Data Pump and an Amazon S3 bucket. The steps are as follows:

1. Export data on the source database using the Oracle DBMS_DATAPUMP package.
2. Place the dump file in an Amazon S3 bucket.
3. Download the dump file from the Amazon S3 bucket to the DATA_PUMP_DIR directory on the target RDS for Oracle DB instance.
4. Import the data from the copied dump file into the RDS for Oracle DB instance using the package DBMS_DATAPUMP.

Topics

- Requirements for Importing data with Oracle Data Pump and an Amazon S3 bucket (p. 1618)
- Step 1: Grant privileges to the database user on the RDS for Oracle target DB instance (p. 1619)
- Step 2: Export data into a dump file using DBMS_DATAPUMP (p. 1619)
- Step 3: Upload the dump file to your Amazon S3 bucket (p. 1620)
- Step 4: Download the dump file from your Amazon S3 bucket to your target DB instance (p. 1621)
- Step 5: Import your dump file into your target DB instance using DBMS_DATAPUMP (p. 1621)
- Step 6: Clean up (p. 1622)

Requirements for Importing data with Oracle Data Pump and an Amazon S3 bucket

The process has the following requirements:

- Make sure that an Amazon S3 bucket is available for file transfers, and that the Amazon S3 bucket is in the same AWS Region as the DB instance. For instructions, see [Create a bucket](#) in the *Amazon Simple Storage Service Getting Started Guide*.
- The object that you upload into the Amazon S3 bucket must be 5 TB or less. For more information about working with objects in Amazon S3, see [Amazon Simple Storage Service User Guide](#).

Note

If your dump file exceeds 5 TB, you can run the Oracle Data Pump export with the parallel option. This operation spreads the data into multiple dump files so that you do not exceed the 5 TB limit for individual files.

- You must prepare the Amazon S3 bucket for Amazon RDS integration by following the instructions in [Configuring IAM permissions for RDS for Oracle integration with Amazon S3 \(p. 1648\)](#).
- You must ensure that you have enough storage space to store the dump file on the source instance and the target DB instance.

Note

This process imports a dump file into the DATA_PUMP_DIR directory, a preconfigured directory on all Oracle DB instances. This directory is located on the same storage volume as your data files. When you import the dump file, the existing Oracle data files use more space. Thus, you should make sure that your DB instance can accommodate that additional use of space. The imported dump file is not automatically deleted or purged from the DATA_PUMP_DIR directory. To remove the imported dump file, use [UTL_FILE.FREMOVE](#), found on the Oracle website.

Step 1: Grant privileges to the database user on the RDS for Oracle target DB instance

In this step, you create the schemas into which you plan to import data and grant the users necessary privileges.

To create users and grant necessary privileges on the RDS for Oracle target instance

1. Use SQL*Plus or Oracle SQL Developer to log in as the master user to the RDS for Oracle DB instance into which the data will be imported. For information about connecting to a DB instance, see [Connecting to your Oracle DB instance \(p. 1488\)](#).
2. Create the required tablespaces before you import the data. For more information, see [Creating and sizing tablespaces \(p. 1544\)](#).
3. Create the user account and grant the necessary permissions and roles if the user account into which the data is imported doesn't exist. If you plan to import data into multiple user schemas, create each user account and grant the necessary privileges and roles to it.

For example, the following SQL statements create a new user and grant the necessary permissions and roles to import the data into the schema owned by this user. Replace `schema_1` with the name of your schema in this step and in the following steps.

```
CREATE USER schema_1 IDENTIFIED BY my_password;
GRANT CREATE SESSION, RESOURCE TO schema_1;
ALTER USER schema_1 QUOTA 100M ON users;
```

The preceding statements grant the new user the CREATE SESSION privilege and the RESOURCE role. You might need additional privileges and roles depending on the database objects that you import.

Step 2: Export data into a dump file using DBMS_DATAPUMP

To create a dump file, use the DBMS_DATAPUMP package.

To export Oracle data into a dump file

1. Use SQL Plus or Oracle SQL Developer to connect to the source RDS for Oracle DB instance with an administrative user. If the source database is an RDS for Oracle DB instance, connect with the Amazon RDS master user.
2. Export the data by calling DBMS_DATAPUMP procedures.

The following script exports the ***SCHEMA_1*** schema into a dump file named `sample.dmp` in the `DATA_PUMP_DIR` directory. Replace ***SCHEMA_1*** with the name of the schema that you want to export.

```

DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(
        operation => 'EXPORT',
        job_mode  => 'SCHEMA',
        job_name   => null
    );
    DBMS_DATAPUMP.ADD_FILE(
        handle    => v_hdnl      ,
        filename  => 'sample.dmp'  ,
        directory => 'DATA_PUMP_DIR',
        filetype  => dbms_datapump.ku$_file_type_dump_file
    );
    DBMS_DATAPUMP.ADD_FILE(
        handle    => v_hdnl,
        filename  => 'sample_exp.log',
        directory => 'DATA_PUMP_DIR',
        filetype  => dbms_datapump.ku$_file_type_log_file
    );
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1''));
    DBMS_DATAPUMP.METADATA_FILTER(
        v_hdnl,
        'EXCLUDE_NAME_EXPR',
        q'[IN (SELECT NAME FROM SYS.OBJ$  

            WHERE TYPE# IN (66,67,74,79,59,62,46)  

            AND OWNER# IN  

                (SELECT USER# FROM SYS.USER$  

                    WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC'))  

            )  

        ]',
        'PROCOBJ'
    );
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/

```

Note

Data Pump starts jobs asynchronously. For information about monitoring a Data Pump job, see [Monitoring job status](#) in the Oracle documentation.

3. (Optional) View the contents of the export log by calling the `rdsadmin.rds_file_util.read_text_file` procedure. For more information, see [Reading files in a DB instance directory \(p. 1598\)](#).

Step 3: Upload the dump file to your Amazon S3 bucket

Use the Amazon RDS procedure `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` to copy the dump file to the Amazon S3 bucket. The following example uploads all of the files from the `DATA_PUMP_DIR` directory to an Amazon S3 bucket named ***myS3bucket***.

```

SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name    => 'myS3bucket',
    p_directory_name => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;

```

The SELECT statement returns the ID of the task in a VARCHAR2 data type. For more information, see [Uploading files from your RDS for Oracle DB instance to an Amazon S3 bucket \(p. 1657\)](#).

Step 4: Download the dump file from your Amazon S3 bucket to your target DB instance

Perform this step using the Amazon RDS procedure

`rdsadmin.rdsadmin_s3_tasks.download_from_s3`. When you download a file to a directory, the procedure `download_from_s3` skips the download if an identically named file already exists in the directory. To remove a file from the download directory, use [UTL_FILE.FREMOVE](#), found on the Oracle website.

To download your dump file

1. Start SQL*Plus or Oracle SQL Developer and log in as the master on your Amazon RDS target Oracle DB instance
2. Download the dump file using the Amazon RDS procedure `rdsadmin.rdsadmin_s3_tasks.download_from_s3`.

The following example downloads all files from an Amazon S3 bucket named `myS3bucket` to the directory `DATA_PUMP_DIR`.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name    => 'myS3bucket',
    p_directory_name => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

The SELECT statement returns the ID of the task in a VARCHAR2 data type. For more information, see [Downloading files from an Amazon S3 bucket to an Oracle DB instance \(p. 1660\)](#).

Step 5: Import your dump file into your target DB instance using DBMS_DATAPUMP

Use DBMS_DATAPUMP to import the schema into your RDS for Oracle DB instance. Additional options such as `METADATA_REMAP` might be required.

To import data into your target DB instance

1. Start SQL*Plus or SQL Developer and log in as the master user to your RDS for Oracle DB instance.
2. Export the data by calling DBMS_DATAPUMP procedures.

The following example imports the `SCHEMA_1` data from `sample_copied.dmp` into your target DB instance.

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(
        operation => 'IMPORT',
        job_mode  => 'SCHEMA',
        job_name   => null);
    DBMS_DATAPUMP.ADD_FILE(
        handle    => v_hdnl,
        filename  => 'sample_copied.dmp',
        directory => 'DATA_PUMP_DIR',
        filetype  => dbms_datapump.ku$_file_type_dump_file);
    DBMS_DATAPUMP.ADD_FILE(
```

```
handle    => v_hdnl,
filename  => 'sample_imp.log',
directory => 'DATA_PUMP_DIR',
filetype   => dbms_datapump.ku$_file_type_log_file);
DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1''));
DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Note

Data Pump jobs are started asynchronously. For information about monitoring a Data Pump job, see [Monitoring job status](#) in the Oracle documentation. You can view the contents of the import log by using the `rdsadmin.rds_file_util.read_text_file` procedure. For more information, see [Reading files in a DB instance directory \(p. 1598\)](#).

3. Verify the data import by listing the schema tables on your target DB instance.

For example, the following query returns the number of tables for `SCHEMA_1`.

```
SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
```

Step 6: Clean up

After the data has been imported, you can delete the files that you don't want to keep.

To remove unneeded files

1. Start SQL*Plus or SQL Developer and log in as the master user to your RDS for Oracle DB instance.
2. List the files in `DATA_PUMP_DIR` using the following command.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY MTIME;
```

3. Delete files in `DATA_PUMP_DIR` that you no longer require, use the following command.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR', 'filename');
```

For example, the following command deletes the file named `sample_copied.dmp`.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR', 'sample_copied.dmp');
```

Importing data with Oracle Data Pump and a database link

The following import process uses Oracle Data Pump and the Oracle `DBMS_FILE_TRANSFER` package. The steps are as follows:

1. Connect to a source Oracle database, which can be an on-premises database, Amazon EC2 instance, or an RDS for Oracle DB instance.
2. Export data using the `DBMS_DATAPUMP` package.
3. Use `DBMS_FILE_TRANSFER.PUT_FILE` to copy the dump file from the Oracle database to the `DATA_PUMP_DIR` directory on the target RDS for Oracle DB instance that is connected using a database link.
4. Import the data from the copied dump file into the RDS for Oracle DB instance using the `DBMS_DATAPUMP` package.

The import process using Oracle Data Pump and the DBMS_FILE_TRANSFER package has the following steps.

Topics

- Requirements for importing data with Oracle Data Pump and a database link (p. 1623)
- Step 1: Grant privileges to the user on the RDS for Oracle target DB instance (p. 1623)
- Step 2: Grant privileges to the user on the source database (p. 1624)
- Step 3: Create a dump file using DBMS_DATAPUMP (p. 1624)
- Step 4: Create a database link to the target DB instance (p. 1625)
- Step 5: Copy the exported dump file to the target DB instance using DBMS_FILE_TRANSFER (p. 1625)
- Step 6: Import the data file to the target DB instance using DBMS_DATAPUMP (p. 1626)
- Step 7: Clean up (p. 1626)

Requirements for importing data with Oracle Data Pump and a database link

The process has the following requirements:

- You must have execute privileges on the DBMS_FILE_TRANSFER and DBMS_DATAPUMP packages.
- You must have write privileges to the DATA_PUMP_DIR directory on the source DB instance.
- You must ensure that you have enough storage space to store the dump file on the source instance and the target DB instance.

Note

This process imports a dump file into the DATA_PUMP_DIR directory, a preconfigured directory on all Oracle DB instances. This directory is located on the same storage volume as your data files. When you import the dump file, the existing Oracle data files use more space. Thus, you should make sure that your DB instance can accommodate that additional use of space. The imported dump file is not automatically deleted or purged from the DATA_PUMP_DIR directory. To remove the imported dump file, use [UTL_FILE.FREMOVE](#), found on the Oracle website.

Step 1: Grant privileges to the user on the RDS for Oracle target DB instance

To grant privileges to the user on the RDS for Oracle target DB instance, take the following steps:

1. Use SQL Plus or Oracle SQL Developer to connect to the RDS for Oracle DB instance into which you intend to import the data. Connect as the Amazon RDS master user. For information about connecting to the DB instance, see [Connecting to your Oracle DB instance \(p. 1488\)](#).
2. Create the required tablespaces before you import the data. For more information, see [Creating and sizing tablespaces \(p. 1544\)](#).
3. If the user account into which the data is imported doesn't exist, create the user account and grant the necessary permissions and roles. If you plan to import data into multiple user schemas, create each user account and grant the necessary privileges and roles to it.

For example, the following commands create a new user named *schema_1* and grant the necessary permissions and roles to import the data into the schema for this user.

```
CREATE USER schema_1 IDENTIFIED BY my-password;
GRANT CREATE SESSION, RESOURCE TO schema_1;
ALTER USER schema_1 QUOTA 100M ON users;
```

The preceding example grants the new user the CREATE SESSION privilege and the RESOURCE role. Additional privileges and roles might be required depending on the database objects that you import.

Note

Replace *schema_1* with the name of your schema in this step and in the following steps.

Step 2: Grant privileges to the user on the source database

Use SQL*Plus or Oracle SQL Developer to connect to the RDS for Oracle DB instance that contains the data to be imported. If necessary, create a user account and grant the necessary permissions.

Note

If the source database is an Amazon RDS instance, you can skip this step. You use your Amazon RDS master user account to perform the export.

The following commands create a new user and grant the necessary permissions.

```
CREATE USER export_user IDENTIFIED BY my-password;
GRANT CREATE SESSION, CREATE TABLE, CREATE DATABASE LINK TO export_user;
ALTER USER export_user QUOTA 100M ON users;
GRANT READ, WRITE ON DIRECTORY data_pump_dir TO export_user;
GRANT SELECT_CATALOG_ROLE TO export_user;
GRANT EXECUTE ON DBMS_DATAPUMP TO export_user;
GRANT EXECUTE ON DBMS_FILE_TRANSFER TO export_user;
```

Step 3: Create a dump file using DBMS_DATAPUMP

To create a dump file, do the following:

1. Use SQL*Plus or Oracle SQL Developer to connect to the source Oracle instance with an administrative user or with the user you created in step 2. If the source database is an Amazon RDS for Oracle DB instance, connect with the Amazon RDS master user.
2. Create a dump file using the Oracle Data Pump utility.

The following script creates a dump file named *sample.dmp* in the DATA_PUMP_DIR directory.

```
DECLARE
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'EXPORT' ,
    job_mode  => 'SCHEMA' ,
    job_name   => null
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample.dmp' ,
    directory => 'DATA_PUMP_DIR' ,
    filetype  => dbms_datapump.ku$_file_type_dump_file
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample_exp.log' ,
    directory => 'DATA_PUMP_DIR' ,
    filetype  => dbms_datapump.ku$_file_type_log_file
  );
  DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl      ,
    'SCHEMA_EXPR' ,
    'IN (''SCHEMA_1'')'
  );
  DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl,
```

```

'EXCLUDE_NAME_EXPR',
q'[IN (SELECT NAME FROM sys.OBJ$  

      WHERE TYPE# IN (66,67,74,79,59,62,46)  

      AND OWNER# IN  

        (SELECT USER# FROM SYS.USER$  

          WHERE NAME IN ('RDSADMIN', 'SYS', 'SYSTEM', 'RDS_DATAGUARD', 'RDSSEC'))  

      )  

    ]',
'PROCOBJ'
);
DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/

```

Note

Data Pump jobs are started asynchronously. For information about monitoring a Data Pump job, see [Monitoring job status](#) in the Oracle documentation. You can view the contents of the export log by using the `rdsadmin.rds_file_util.read_text_file` procedure. For more information, see [Reading files in a DB instance directory \(p. 1598\)](#).

Step 4: Create a database link to the target DB instance

Create a database link between your source DB instance and your target DB instance. Your local Oracle instance must have network connectivity to the DB instance in order to create a database link and to transfer your export dump file.

Perform this step connected with the same user account as the previous step.

If you are creating a database link between two DB instances inside the same VPC or peered VPCs, the two DB instances should have a valid route between them. The security group of each DB instance must allow ingress to and egress from the other DB instance. The security group inbound and outbound rules can refer to security groups from the same VPC or a peered VPC. For more information, see [Adjusting database links for use with DB instances in a VPC \(p. 1553\)](#).

The following command creates a database link named `to_rds` that connects to the Amazon RDS master user at the target DB instance.

```

CREATE DATABASE LINK to_rds
  CONNECT TO <master_user_account> IDENTIFIED BY <password>
  USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns or ip address of remote db>)
    (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))';

```

Step 5: Copy the exported dump file to the target DB instance using DBMS_FILE_TRANSFER

Use `DBMS_FILE_TRANSFER` to copy the dump file from the source database instance to the target DB instance. The following script copies a dump file named `sample.dmp` from the source instance to a target database link named `to_rds` (created in the previous step).

```

BEGIN
  DBMS_FILE_TRANSFER.PUT_FILE(
    source_directory_object    => 'DATA_PUMP_DIR',
    source_file_name           => 'sample.dmp',
    destination_directory_object => 'DATA_PUMP_DIR',
    destination_file_name      => 'sample_copied.dmp',
    destination_database        => 'to_rds' );
END;
/

```

Step 6: Import the data file to the target DB instance using DBMS_DATAPUMP

Use Oracle Data Pump to import the schema in the DB instance. Additional options such as METADATA_REMAP might be required.

Connect to the DB instance with the Amazon RDS master user account to perform the import.

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(
        operation => 'IMPORT',
        job_mode  => 'SCHEMA',
        job_name   => null);
    DBMS_DATAPUMP.ADD_FILE(
        handle    => v_hdnl,
        filename  => 'sample_copied.dmp',
        directory => 'DATA_PUMP_DIR',
        filetype  => dbms_datapump.ku$_file_type_dump_file );
    DBMS_DATAPUMP.ADD_FILE(
        handle    => v_hdnl,
        filename  => 'sample_imp.log',
        directory => 'DATA_PUMP_DIR',
        filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1''));
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Note

Data Pump jobs are started asynchronously. For information about monitoring a Data Pump job, see [Monitoring job status](#) in the Oracle documentation. You can view the contents of the import log by using the `rdsadmin.rds_file_util.read_text_file` procedure. For more information, see [Reading files in a DB instance directory \(p. 1598\)](#).

You can verify the data import by viewing the user's tables on the DB instance. For example, the following query returns the number of tables for `schema_1`.

```
SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
```

Step 7: Clean up

After the data has been imported, you can delete the files that you don't want to keep. You can list the files in DATA_PUMP_DIR using the following command.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY MTIME;
```

To delete files in DATA_PUMP_DIR that you no longer require, use the following command.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR', '<file name>');
```

For example, the following command deletes the file named "sample_copied.dmp".

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR', 'sample_copied.dmp');
```

Importing using Oracle Export/Import

You might consider Oracle Export/Import utilities for migrations in the following conditions:

- Your data size is small.
- Data types such as binary float and double aren't required.

The import process creates the necessary schema objects, so you don't need to run a script to create the objects beforehand. To download Oracle export and import utilities, go to <http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html>.

To export tables and then import them

1. Export the tables from the source database using the `exp` command.

The following command exports the tables named `tab1`, `tab2`, and `tab3`. The dump file is `exp_file.dmp`.

```
exp cust_dba@ORCL FILE=exp_file.dmp TABLES=(tab1,tab2,tab3) LOG=exp_file.log
```

The export creates a binary dump file that contains both the schema and data for the specified tables.

2. Import the schema and data into a target database using the `imp` command.

The following command imports the tables `tab1`, `tab2`, and `tab3` from dump file `exp_file.dmp`.

```
imp cust_dba@targetdb FROMUSER=cust_schema TOUSER=cust_schema \
TABLES=(tab1,tab2,tab3) FILE=exp_file.dmp LOG=imp_file.log
```

Export and Import have other variations that might be better suited to your requirements. See the Oracle Database documentation for full details.

Importing using Oracle SQL*Loader

You might consider Oracle SQL*Loader for large databases that contain a limited number of objects. Because the process of exporting from a source database and loading to a target database is specific to the schema, the following example creates the sample schema objects, exports from a source, and then loads the data into a target database.

To download Oracle SQL*Loader, go to <http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html>.

1. Create a sample source table using the following SQL statement.

```
CREATE TABLE customer_0 TABLESPACE users
AS (SELECT ROWNUM id, o.*
     FROM ALL_OBJECTS o, ALL_OBJECTS x
    WHERE ROWNUM <= 1000000);
```

2. On the target RDS for Oracle DB instance, create a destination table for loading the data. The clause `WHERE 1=2` ensures that you copy the structure of `ALL_OBJECTS`, but don't copy any rows.

```
CREATE TABLE customer_1 TABLESPACE users
AS (SELECT 0 AS ID, OWNER, OBJECT_NAME, CREATED
     FROM ALL_OBJECTS
    WHERE 1=2);
```

3. Export the data from the source database to a text file. The following example uses SQL*Plus. For your data, you will likely need to generate a script that does the export for all the objects in the database.

```
ALTER SESSION SET NLS_DATE_FORMAT = 'YYYY/MM/DD HH24:MI:SS'

SET LINESIZE 800 HEADING OFF FEEDBACK OFF ARRAY 5000 PAGESIZE 0
SPOOL customer_0.out
SET MARKUP HTML PREFORMAT ON
SET COLSEP ','

SELECT id, owner, object_name, created
FROM   customer_0;

SPOOL OFF
```

4. Create a control file to describe the data. You might need to write a script to perform this step.

```
cat << EOF > sqlldr_1.ctl
load data
infile customer_0.out
into table customer_1
APPEND
fields terminated by "," optionally enclosed by "'"
(
  id          POSITION(01:10)      INTEGER EXTERNAL,
  owner       POSITION(12:41)      CHAR,
  object_name POSITION(43:72)      CHAR,
  created     POSITION(74:92)      date "YYYY/MM/DD HH24:MI:SS"
)
```

If needed, copy the files generated by the preceding code to a staging area, such as an Amazon EC2 instance.

5. Import the data using SQL*Loader with the appropriate user name and password for the target database.

```
sqlldr cust_dba@targetdb CONTROL=sqlldr_1.ctl BINDSIZE=10485760 READSIZE=10485760
ROWS=1000
```

Migrating with Oracle materialized views

To migrate large datasets efficiently, you can use Oracle materialized view replication. With replication, you can keep the target tables synchronized with the source tables. Thus, you can switch over to Amazon RDS later, if needed.

Before you can migrate using materialized views, make sure that you meet the following requirements:

- Configure access from the target database to the source database. In the following example, access rules were enabled on the source database to allow the RDS for Oracle target database to connect to the source over SQL*Net.
- Create a database link from the RDS for Oracle DB instance to the source database.

To migrate data using materialized views

1. Create a user account on both source and RDS for Oracle target instances that can authenticate with the same password. The following example creates a user named dblink_user.

```
CREATE USER dblink_user IDENTIFIED BY my-password
  DEFAULT TABLESPACE users
  TEMPORARY TABLESPACE temp;

GRANT CREATE SESSION TO dblink_user;

GRANT SELECT ANY TABLE TO dblink_user;

GRANT SELECT ANY DICTIONARY TO dblink_user;
```

2. Create a database link from the RDS for Oracle target instance to the source instance using your newly created user.

```
CREATE DATABASE LINK remote_site
  CONNECT TO dblink_user IDENTIFIED BY my-password
  USING '(description=(address=(protocol=tcp) (host=my-host)
  (port=my-listener-port)) (connect_data=(sid=my-source-db-sid)))';
```

3. Test the link:

```
SELECT * FROM V$INSTANCE@remote_site;
```

4. Create a sample table with primary key and materialized view log on the source instance.

```
CREATE TABLE customer_0 TABLESPACE users
  AS (SELECT ROWNUM id, o.*
      FROM ALL_OBJECTS o, ALL_OBJECTS x
     WHERE ROWNUM <= 1000000);

ALTER TABLE customer_0 ADD CONSTRAINT pk_customer_0 PRIMARY KEY (id) USING INDEX;

CREATE MATERIALIZED VIEW LOG ON customer_0;
```

5. On the target RDS for Oracle DB instance, create a materialized view.

```
CREATE MATERIALIZED VIEW customer_0
  BUILD IMMEDIATE REFRESH FAST
  AS (SELECT *
      FROM cust_dba.customer_0@remote_site);
```

6. On the target RDS for Oracle DB instance, refresh the materialized view.

```
EXEC DBMS_MV.REFRESH('CUSTOMER_0', 'f');
```

7. Drop the materialized view and include the PRESERVE TABLE clause to retain the materialized view container table and its contents.

```
DROP MATERIALIZED VIEW customer_0 PRESERVE TABLE;
```

The retained table has the same name as the dropped materialized view.

Working with read replicas for Amazon RDS for Oracle

To configure replication between Oracle DB instances, you can create replica databases. For an overview of Amazon RDS read replicas, see [Overview of Amazon RDS read replicas \(p. 372\)](#). For a summary of the differences between Oracle replicas and other DB engines, see [Differences between read replicas for different DB engines \(p. 373\)](#).

Topics

- [Overview of RDS for Oracle replicas \(p. 1630\)](#)
- [Considerations for RDS for Oracle replicas \(p. 1631\)](#)
- [Preparing to create an Oracle replica \(p. 1633\)](#)
- [Creating an RDS for Oracle replica in mounted mode \(p. 1634\)](#)
- [Modifying the RDS for Oracle replica mode \(p. 1636\)](#)
- [Working with RDS for Oracle replica backups \(p. 1636\)](#)
- [Performing an Oracle Data Guard switchover \(p. 1638\)](#)
- [Troubleshooting RDS for Oracle replicas \(p. 1644\)](#)

Overview of RDS for Oracle replicas

An *Oracle replica* database is a physical copy of your primary database. An Oracle replica in read-only mode is called a *read replica*. An Oracle replica in mounted mode is called a *mounted replica*. Oracle Database doesn't permit writes in a replica, but you can promote a replica to make it writable. The promoted read replica has the replicated data to the point when the request was made to promote it.

The following video provides a helpful overview of RDS for Oracle disaster recovery.

For more information, see the blog post [Managed disaster recovery with Amazon RDS for Oracle cross-Region automated backups - Part 1](#) and [Managed disaster recovery with Amazon RDS for Oracle cross-Region automated backups - Part 2](#).

Topics

- [Read-only and mounted replicas \(p. 1630\)](#)
- [Archived redo log retention \(p. 1631\)](#)
- [Outages during replication \(p. 1631\)](#)

Read-only and mounted replicas

When creating or modifying an Oracle replica, you can place it in either of the following modes:

Read-only

This is the default. Active Data Guard transmits and applies changes from the source database to all read replica databases.

You can create up to five read replicas from one source DB instance. For general information about read replicas that applies to all DB engines, see [Working with read replicas \(p. 370\)](#). For information about Oracle Data Guard, see [Oracle Data Guard concepts and administration](#) in the Oracle documentation.

Mounted

In this case, replication uses Oracle Data Guard, but the replica database doesn't accept user connections. The primary use for mounted replicas is cross-Region disaster recovery.

A mounted replica can't serve a read-only workload. The mounted replica deletes archived redo log files after it applies them, regardless of the archived log retention policy.

You can create a combination of mounted and read-only DB replicas for the same source DB instance. You can change a read-only replica to mounted mode, or change a mounted replica to read-only mode. In either case, the Oracle database preserves the archived log retention setting.

Archived redo log retention

If a primary DB instance has no cross-Region read replicas, Amazon RDS for Oracle keeps a minimum of two hours of archived redo logs on the source DB instance. This is true regardless of the setting for `archivelog retention hours` in `rdsadmin.rdsadmin_util.set_configuration`.

RDS purges logs from the source DB instance after two hours or after the archive log retention hours setting has passed, whichever is longer. RDS purges logs from the read replica after the archive log retention hours setting has passed only if they have been successfully applied to the database.

In some cases, a primary DB instance might have one or more cross-Region read replicas. If so, Amazon RDS for Oracle keeps the transaction logs on the source DB instance until they have been transmitted and applied to all cross-Region read replicas. For information about `rdsadmin.rdsadmin_util.set_configuration`, see [Retaining archived redo logs \(p. 1564\)](#).

Outages during replication

When you create an Oracle replica, no outage occurs for the source DB instance. Amazon RDS takes a snapshot of the source DB instance. This snapshot becomes the replica. Amazon RDS sets the necessary parameters and permissions for the source DB and replica without service interruption. Similarly, if you delete a replica, no outage occurs.

Considerations for RDS for Oracle replicas

Before creating an Oracle replica, consider the following requirements, restrictions, and recommendations.

Topics

- [Version and licensing considerations for RDS for Oracle replicas \(p. 1631\)](#)
- [Option considerations for RDS for Oracle replicas \(p. 1632\)](#)
- [Backup and restore considerations for RDS for Oracle replicas \(p. 1632\)](#)
- [Miscellaneous considerations for RDS for Oracle replicas \(p. 1633\)](#)

Version and licensing considerations for RDS for Oracle replicas

Before you create an RDS for Oracle replica, consider the following requirements, restrictions, and recommendations:

- If the replica is in read-only mode, make sure that you have an Active Data Guard license. If you place the replica in mounted mode, you don't need an Active Data Guard license. Only the Oracle DB engine supports mounted replicas.
- Oracle replicas are supported for the Oracle Enterprise Edition (EE) engine only.

- Oracle replicas are available for instances created using version Oracle Database 12c Release 1 (12.1.0.2.v10) and higher 12c releases, and for non-CDB instances of Oracle Database 19c. Replicas of CDBs aren't supported.
- Oracle replicas are available for DB instances running only on DB instance classes with two or more vCPUs. A source DB instance can't use the db.t3.micro or db.t3.small instance classes.
- The Oracle DB engine version of the source DB instance and all of its replicas must be the same. Amazon RDS upgrades the replicas immediately after upgrading the source DB instance, regardless of a replica's maintenance window. For major version upgrades of cross-Region replicas, Amazon RDS automatically does the following:
 - Generates an option group for the target version.
 - Copies all options and option settings from the original option group to the new option group.
 - Associates the upgraded cross-Region replica with the new option group.

For more information about upgrading the DB engine version, see [Upgrading the RDS for Oracle DB engine \(p. 1757\)](#).

Option considerations for RDS for Oracle replicas

Before you create an RDS for Oracle replica, consider the following requirements, restrictions, and recommendations:

- If your Oracle replica is in the same AWS Region as its source DB instance, make sure that it belongs to the same option group as the source DB instance. Modifications to the source option group or source option group membership propagate to replicas. These changes are applied to the replicas immediately after they are applied to the source DB instance, regardless of the replica's maintenance window.

For more information about option groups, see [Working with option groups \(p. 273\)](#).

- When you create an Oracle cross-Region replica, Amazon RDS creates a dedicated option group for it.

You can't remove an Oracle cross-Region replica from its dedicated option group. No other DB instances can use the dedicated option group for an Oracle cross-Region replica.

You can only add or remove the following nonreplicated options from a dedicated option group:

- NATIVE_NETWORK_ENCRYPTION
- OEM
- OEM_AGENT
- SSL

To add other options to an Oracle cross-Region replica, add them to the source DB instance's option group. The option is also installed on all of the source DB instance's replicas. For licensed options, make sure that there are sufficient licenses for the replicas.

When you promote an Oracle cross-Region replica, the promoted replica behaves the same as other Oracle DB instances, including the management of its options. You can promote a replica explicitly or implicitly by deleting its source DB instance.

For more information about option groups, see [Working with option groups \(p. 273\)](#).

Backup and restore considerations for RDS for Oracle replicas

Before you create an RDS for Oracle replica, consider the following requirements, restrictions, and recommendations:

- To create snapshots of RDS for Oracle replicas or turn on automatic backups, make sure to set the backup retention period manually. Automatic backups aren't turned on by default.
- The *database time* refers to the latest applied transaction time of the data in the backup. When you restore a replica backup, you restore to the database time, not the time that the backup was taken. The difference is significant because a replica can lag behind the primary for minutes or hours.

To find the difference, use the `describe-db-snapshots` command. Compare the `snapshotDatabaseTime`, which is the database time of the replica backup, and the `OriginalSnapshotCreateTime` field, which is the latest applied transaction on the primary database.

Miscellaneous considerations for RDS for Oracle replicas

Before you create an RDS for Oracle replica, consider the following requirements, restrictions, and recommendations:

- If a DB instance is a source for one or more cross-Region replicas, the source DB retains its archived redo logs until they are applied on all cross-Region replicas. The archived redo logs might result in increased storage consumption.
- A logon trigger on a primary instance must permit access to the `RDS_DATAGUARD` user and to any user whose `AUTHENTICATED_IDENTITY` value is `RDS_DATAGUARD` or `rdsdb`. Also, the trigger must not set the current schema for the `RDS_DATAGUARD` user.
- To avoid disrupting RDS automation, system triggers must permit specific users to log on to the primary and replica database. [System triggers](#) include DDL, logon, and database role triggers. We recommend that you add code to your triggers to exclude the users listed in the following sample code:

```
-- Determine who the user is
SELECT SYS_CONTEXT('USERENV', 'AUTHENTICATED_IDENTITY') INTO CURRENT_USER FROM DUAL;
-- The following users should always be able to login to either the Primary or Replica
IF CURRENT_USER IN ('master_user', 'SYS', 'SYSTEM', 'RDS_DATAGUARD', 'rdsdb') THEN
RETURN;
END IF;
```

- To avoid blocking connections from the Data Guard broker process, don't enable restricted sessions. For more information about restricted sessions, see [Enabling and disabling restricted sessions \(p. 1532\)](#).
- Block change tracking is supported for read-only replicas, but not for mounted replicas. You can change a mounted replica to a read-only replica, and then enable block change tracking. For more information, see [Enabling and disabling block change tracking \(p. 1574\)](#).

Preparing to create an Oracle replica

Before you can begin using your replica, perform the following tasks.

Topics

- [Enabling automatic backups \(p. 1634\)](#)
- [Enabling force logging mode \(p. 1634\)](#)
- [Changing your logging configuration \(p. 1634\)](#)
- [Setting the MAX_STRING_SIZE parameter \(p. 1634\)](#)
- [Planning compute and storage resources \(p. 1634\)](#)

Enabling automatic backups

Before a DB instance can serve as a source DB instance, make sure to enable automatic backups on the source DB instance. To learn how to perform this procedure, see [Enabling automated backups \(p. 429\)](#).

Enabling force logging mode

We recommend that you enable force logging mode. In force logging mode, the Oracle database writes redo records even when NOLOGGING is used with data definition language (DDL) statements.

To enable force logging mode

1. Log in to your Oracle database using a client tool such as SQL Developer.
2. Enable force logging mode by running the following procedure.

```
exec rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

For more information about this procedure, see [Setting force logging \(p. 1560\)](#).

Changing your logging configuration

If you want to change your logging configuration, we recommend that you complete the changes before making a DB instance the source for replicas. Also, we recommend that you not modify the logging configuration after you create the replicas. Modifications can cause the online redo logging configuration to get out of sync with the standby logging configuration.

Modify the logging configuration for a DB instance by using the Amazon RDS procedures `rdsadmin.rdsadmin_util.add_logfile` and `rdsadmin.rdsadmin_util.drop_logfile`. For more information, see [Adding online redo logs \(p. 1562\)](#) and [Dropping online redo logs \(p. 1562\)](#).

Setting the MAX_STRING_SIZE parameter

Before you create an Oracle replica, ensure that the setting of the MAX_STRING_SIZE parameter is the same on the source DB instance and the replica. You can do this by associating them with the same parameter group. If you have different parameter groups for the source and the replica, you can set MAX_STRING_SIZE to the same value. For more information about setting this parameter, see [Turning on extended data types for a new DB instance \(p. 1613\)](#).

Planning compute and storage resources

Ensure that the source DB instance and its replicas are sized properly, in terms of compute and storage, to suit their operational load. If a replica reaches compute, network, or storage resource capacity, the replica stops receiving or applying changes from its source. Amazon RDS for Oracle doesn't intervene to mitigate high replica lag between a source DB instance and its replicas. You can modify the storage and CPU resources of a replica independently from its source and other replicas.

Creating an RDS for Oracle replica in mounted mode

By default, Oracle replicas are read-only. To create a replica in mounted mode, use the console, the AWS CLI, or the RDS API.

Console

To create a mounted replica from a source Oracle DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the Oracle DB instance that you want to use as the source for a mounted replica.
4. For **Actions**, choose **Create replica**.
5. For **Replica mode**, choose **Mounted**.
6. Choose the settings that you want to use. For **DB instance identifier**, enter a name for the read replica. Adjust other settings as needed.
7. For **Regions**, choose the Region where the mounted replica will be launched.
8. Choose your instance size and storage type. We recommend that you use the same DB instance class and storage type as the source DB instance for the read replica.
9. For **Multi-AZ deployment**, choose **Create a standby instance** to create a standby of your replica in another Availability Zone for failover support for the mounted replica. Creating your mounted replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.
10. Choose the other settings that you want to use.
11. Choose **Create replica**.

In the **Databases** page, the mounted replica has the role **Replica**.

AWS CLI

To create an Oracle replica in mounted mode, set **--replica-mode** to **mounted** in the AWS CLI command [create-db-instance-read-replica](#).

Example

For Linux, macOS, or Unix:

```
aws rds create-db-instance-read-replica \
  --db-instance-identifier myreadreplica \
  --source-db-instance-identifier mydbinstance \
  --replica-mode mounted
```

For Windows:

```
aws rds create-db-instance-read-replica ^
  --db-instance-identifier myreadreplica ^
  --source-db-instance-identifier mydbinstance ^
  --replica-mode mounted
```

To change a read-only replica to a mounted state, set **--replica-mode** to **mounted** in the AWS CLI command [modify-db-instance](#). To place a mounted replica in read-only mode, set **--replica-mode** to **open-read-only**.

RDS API

To create an Oracle replica in mounted mode, specify **ReplicaMode=mounted** in the RDS API operation [CreateDBInstanceReadReplica](#).

Modifying the RDS for Oracle replica mode

To change the replica mode of an existing replica, use the console, AWS CLI, or RDS API. When you change to mounted mode, the replica disconnects all active connections. When you change to read-only mode, Amazon RDS initializes Active Data Guard.

The change operation can take a few minutes. During the operation, the DB instance status changes to **modifying**. For more information about status changes, see [Viewing Amazon RDS DB instance status \(p. 516\)](#).

Console

To change the replica mode of an Oracle replica from mounted to read-only

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the mounted replica database.
4. Choose **Modify**.
5. For **Replica mode**, choose **Read-only**.
6. Choose the other settings that you want to change.
7. Choose **Continue**.
8. For **Scheduling of modifications**, choose **Apply immediately**.
9. Choose **Modify DB instance**.

AWS CLI

To change a read replica to mounted mode, set `--replica-mode` to `mounted` in the AWS CLI command `modify-db-instance`. To change a mounted replica to read-only mode, set `--replica-mode` to `open-read-only`.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier myreadreplica \
  --replica-mode mode
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier myreadreplica ^
  --replica-mode mode
```

RDS API

To change a read-only replica to mounted mode, set `ReplicaMode=mounted` in `ModifyDBInstance`. To change a mounted replica to read-only mode, set `ReplicaMode=read-only`.

Working with RDS for Oracle replica backups

You can create and restore backups of an RDS for Oracle replica. Both automatic backups and manual snapshots are supported. For more information, see [Backing up and restoring an Amazon RDS DB](#)

instance (p. 426). The following sections describe the key differences between managing backups of a primary and an RDS for Oracle replica.

Turning on RDS for Oracle replica backups

An Oracle replica doesn't have automated backups turned on by default. You turn on automated backups by setting the backup retention period to a positive nonzero value.

Console

To enable automated backups immediately

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**. The **Modify DB instance** page appears.
4. For **Backup retention period**, choose a positive nonzero value, for example 3 days.
5. Choose **Continue**.
6. Choose **Apply immediately**.
7. On the confirmation page, choose **Modify DB instance** to save your changes and enable automated backups.

AWS CLI

To enable automated backups, use the AWS CLI `modify-db-instance` command.

Include the following parameters:

- `--db-instance-identifier`
- `--backup-retention-period`
- `--apply-immediately` or `--no-apply-immediately`

In the following example, we enable automated backups by setting the backup retention period to three days. The changes are applied immediately.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --backup-retention-period 3 \
  --apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --backup-retention-period 3 ^
  --apply-immediately
```

RDS API

To enable automated backups, use the RDS API [ModifyDBInstance](#) operation with the following required parameters:

- `DBInstanceIdentifier`
- `BackupRetentionPeriod`

Restoring an RDS for Oracle replica backup

You can restore an Oracle replica backup just as you can restore a backup of the primary instance. For more information, see the following:

- [Restoring from a DB snapshot \(p. 452\)](#)
- [Restoring a DB instance to a specified time \(p. 499\)](#)

The main consideration when you restore a replica backup is determining the point in time to which you are restoring. The *database time* refers to the latest applied transaction time of the data in the backup. When you restore a replica backup, you restore to the database time, not the time when the backup completed. The difference is significant because an RDS for Oracle replica can lag behind the primary by minutes or hours. Thus, the database time of a replica backup, and thus the point in time to which you restore it, might be much earlier than the backup creation time.

To find the difference between database time and creation time, use the `describe-db-snapshots` command. Compare the `SnapshotDatabaseTime`, which is the database time of the replica backup, and the `OriginalSnapshotCreateTime` field, which is the latest applied transaction on the primary database. The following example shows the difference between the two times:

```
aws rds describe-db-snapshots \
    --db-instance-identifier my-oracle-replica
    --db-snapshot-identifier my-replica-snapshot

{
    "DBSnapshots": [
        {
            "DBSnapshotIdentifier": "my-replica-snapshot",
            "DBInstanceIdentifier": "my-oracle-replica",
            "SnapshotDatabaseTime": "2022-07-26T17:49:44Z",
            ...
            "OriginalSnapshotCreateTime": "2021-07-26T19:49:44Z"
        }
    ]
}
```

Performing an Oracle Data Guard switchover

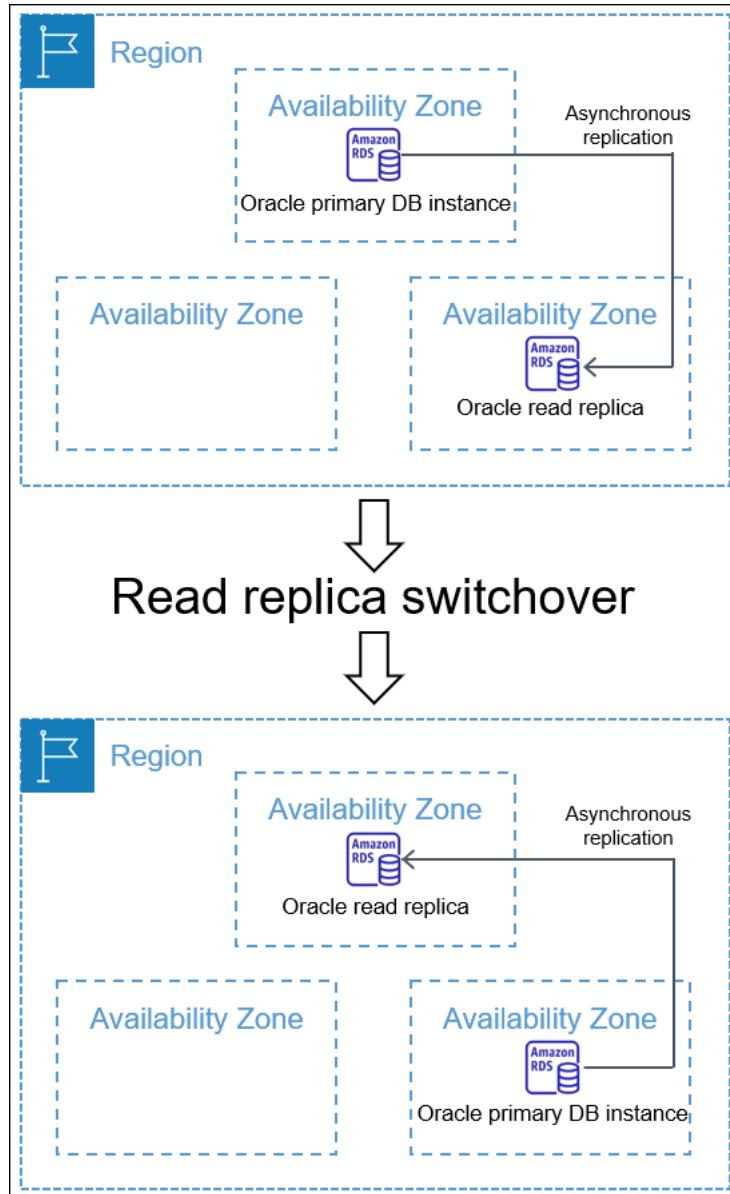
In an Oracle Data Guard environment, a primary database supports one or more standby databases. You can perform a managed, switchover-based role transition from a primary database to a standby database.

Topics

- [Overview of Oracle Data Guard switchover \(p. 1639\)](#)
- [Preparing for the Oracle Data Guard switchover \(p. 1642\)](#)
- [Initiating the Oracle Data Guard switchover \(p. 1642\)](#)
- [Monitoring the Oracle Data Guard switchover \(p. 1643\)](#)

Overview of Oracle Data Guard switchover

A *switchover* is a role reversal between a primary database and a standby database. During a switchover, the original primary database transitions to a standby role, while the original standby database transitions to the primary role.



Amazon RDS supports a fully managed, switchover-based role transition for Oracle Database replicas. The replicas can reside in separate AWS Regions or in different Availability Zones (AZs) of a single Region. You can only initiate a switchover to a standby database that is mounted or open read-only.

Topics

- [Benefits of Oracle Data Guard switchover \(p. 1640\)](#)
- [Supported Oracle Database versions \(p. 1640\)](#)
- [AWS Region support \(p. 1640\)](#)
- [Cost of Oracle Data Guard switchover \(p. 1640\)](#)

- [How Oracle Data Guard switchover works \(p. 1641\)](#)

Benefits of Oracle Data Guard switchover

Just as for RDS for Oracle read replicas, a managed switchover relies on Oracle Data Guard. The operation is designed to have zero data loss. Amazon RDS automates the following aspects of the switchover:

- Reverses the roles of your primary database and specified standby database, putting the new standby database in the same state (mounted or read-only) as the original standby
- Ensures data consistency
- Maintains your replication configuration after the transition
- Supports repeated reversals, allowing your new standby database to return to its original primary role

Supported Oracle Database versions

Oracle Data Guard switchover is supported for the following releases:

- Oracle Database 19c
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1) using PSU 12.1.0.2.v10 or higher

AWS Region support

Oracle Data Guard switchover is available in the following AWS Regions:

- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

Cost of Oracle Data Guard switchover

The Oracle Data Guard switchover feature doesn't incur additional costs. You need an Oracle Data Guard license to use read replicas in mounted mode, and an Oracle Active Data Guard license to use read replicas in read-only mode.

How Oracle Data Guard switchover works

Oracle Data Guard switchover is a fully managed operation. You initiate the switchover for a standby database by issuing the CLI command `switchover-read-replica`. Then Amazon RDS modifies the primary and standby roles in your replication configuration.

The *original standby* and *original primary* are the roles that exist before the switchover. The *new standby* and *new primary* are the roles that exist after the switchover. A *bystander replica* is a replica database that serves as a standby database in the Oracle Data Guard environment but is not switching roles.

Topics

- [Stages of the Oracle Data Guard switchover \(p. 1641\)](#)
- [After the Oracle Data Guard switchover \(p. 1641\)](#)

Stages of the Oracle Data Guard switchover

To perform the switchover, Amazon RDS must take the following steps:

1. Block new transactions on the original primary database. During the switchover, Amazon RDS interrupts replication for all databases in your Oracle Data Guard configuration. During the switchover, the original primary database can't process write requests.
2. Ship unapplied transactions to the original standby database, and apply them.
3. Restart the new standby database in read-only or mounted mode. The mode depends on the open state of the original standby database before the switchover.
4. Open the new primary database in read/write mode.

After the Oracle Data Guard switchover

Amazon RDS switches the roles of the primary and standby database. You are responsible for reconnecting your application and performing any other desired configuration.

Topics

- [Success criteria \(p. 1641\)](#)
- [Connection to the new primary database \(p. 1641\)](#)
- [Configuration of the new primary database \(p. 1642\)](#)

Success criteria

The Oracle Data Guard switchover is successful when the original standby database does the following:

- Transitions to its role as new primary database
- Completes its reconfiguration

To limit downtime, your new primary database becomes active as soon as possible. Because Amazon RDS configures bystander replicas asynchronously, these replicas might become active after the original primary database.

Connection to the new primary database

Amazon RDS won't propagate your current database connections to the new primary database after the switchover. After the Oracle Data Guard switchover completes, reconnect your application to the new primary database.

Configuration of the new primary database

To perform a switchover to the new primary database, Amazon RDS changes the mode of the original standby database to open. The change in role is the only change to the database. Amazon RDS doesn't set up features such as Multi-AZ replication.

If you perform a switchover to a cross-Region replica with different options, the new primary database keeps its own options. Amazon RDS won't migrate the options on the original primary database. If the original primary database had options such as SSL, NNE, OEM, and OEM_AGENT, Amazon RDS doesn't propagate them to the new primary database.

Preparing for the Oracle Data Guard switchover

Before initiating the Oracle Data Guard switchover, make sure that your replication environment meets the following requirements:

- The original standby database is mounted or open read-only.
- Automatic backups are enabled on the original standby database.
- The original primary database and the original standby database are in an available state.
- The original primary database and the original standby database have no pending maintenance actions.
- The original standby database is in the replicating state.
- You aren't attempting to initiate a switchover when either the primary database or standby database is currently in a switchover lifecycle. If a replica database is reconfiguring after a switchover, Amazon RDS prevents you from initiating another switchover.

Note

A *bystander replica* is a replica in the Oracle Data Guard configuration that isn't the target of the switchover. Bystander replicas can be in any state during the switchover.

- The original standby database has a configuration that is as close as desired to the original primary database. Assume a scenario where the original primary and original standby databases have different options. After the switchover completes, Amazon RDS doesn't automatically reconfigure the new primary database to have the same options as the original primary database.
- You configure your desired Multi-AZ deployment before initiating a switchover. Amazon RDS doesn't manage Multi-AZ as part of the switchover. The Multi-AZ deployment remains as it is.

Assume that db_maz is the primary database in a Multi-AZ deployment, and db_saz is a Single-AZ replica. You initiate a switchover from db_maz to db_saz. Afterward, db_maz is a Multi-AZ replica database, and db_saz is a Single-AZ primary database. The new primary database is now unprotected by a Multi-AZ deployment.

- In preparation for a cross-Region switchover, the primary database doesn't use the same option group as a DB instance outside of the replication configuration. For a cross-Region switchover to succeed, the current primary database and its read replicas must be the only DB instances to use the option group of the current primary database. Otherwise, Amazon RDS prevents the switchover.

Initiating the Oracle Data Guard switchover

You can switch over an RDS for Oracle read replica to the primary role, and the former primary DB instance to a replica role.

Console

To switch over an Oracle read replica to the primary DB role

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the Amazon RDS console, choose **Databases**.

The **Databases** pane appears. Each read replica shows **Replica** in the **Role** column.

3. Choose the read replica that you want to switch over to the primary role.
4. For **Actions**, choose **Switch over replica**.
5. Choose **I acknowledge**. Then choose **Switch over replica**.
6. On the **Databases** page, monitor the progress of the switchover.

The screenshot shows the 'Databases' section of the Amazon RDS console. A modal dialog at the top states: 'Switch over replica is in progress for database-2.' It explains that the switchover is in progress for database-2, replication is interrupted, and RDS is restarting the old and new primary databases and transferring transactions to database-2. A 'View details' button is in the top right of the modal. Below the modal, the main table lists two databases:

DB identifier	Role	Engine	Region & AZ	Size	Status
database-1	Replica	Oracle Enterprise Edition	us-east-2a	db.m5.xlarge	Available
database-2	Replica	Oracle Enterprise Edition	us-east-2a	db.m5.xlarge	Modifying

When the switchover completes, the role of the switchover target changes from **Replica** to **Primary**.

AWS CLI

To switch over an Oracle replica to the primary DB role, use the AWS CLI [switchover-read-replica](#) command. The following examples make the Oracle replica named *replica-to-be-made-primary* into the new primary database.

Example

For Linux, macOS, or Unix:

```
aws rds switchover-read-replica \
--db-instance-identifier replica-to-be-made-primary
```

For Windows:

```
aws rds switchover-read-replica ^
--db-instance-identifier replica-to-be-made-primary
```

RDS API

To switch over an Oracle replica to the primary DB role, call the Amazon RDS API [SwitchoverReadReplica](#) operation with the required parameter `DBInstanceIdentifier`. This parameter specifies the name of the Oracle replica that you want to assume the primary DB role.

Monitoring the Oracle Data Guard switchover

To check the status of your instances, use the AWS CLI command `describe-db-instances`. The following command checks the status of the DB instance *orcl2*. This database was a standby database before the switchover, but is the new primary database after the switchover.

```
aws rds describe-db-instances \
--db-instance-identifier orcl2
```

To confirm that the switchover completed successfully, query V\$DATABASE.OPEN_MODE. Check that the value for the new primary database is READ WRITE.

```
SELECT OPEN_MODE FROM V$DATABASE;
```

To look for switchover-related events, use the AWS CLI command `describe-events`. The following example looks for events on the `orcl2` instance.

```
aws rds describe-events \
--source-identifier orcl2 \
--source-type db-instance
```

Troubleshooting RDS for Oracle replicas

This section describes possible replication problems and solutions.

Topics

- [Monitoring Oracle replication lag \(p. 1644\)](#)
- [Troubleshooting Oracle replication failure after adding or modifying triggers \(p. 1644\)](#)

Monitoring Oracle replication lag

To monitor replication lag in Amazon CloudWatch, view the Amazon RDS ReplicaLag metric. For more information about replication lag time, see [Monitoring read replication \(p. 380\)](#) and [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).

For a read replica, if the lag time is too long, query the following views:

- V\$ARCHIVED_LOG – Shows which commits have been applied to the read replica.
- V\$DATAGUARD_STATS – Shows a detailed breakdown of the components that make up the ReplicaLag metric.
- V\$DATAGUARD_STATUS – Shows the log output from Oracle's internal replication processes.

For a mounted replica, if the lag time is too long, you can't query the V\$ views. Instead, do the following:

- Check the ReplicaLag metric in CloudWatch.
- Check the alert log file for the replica in the console. Look for errors in the recovery messages. The messages include the log sequence number, which you can compare to the primary sequence number. For more information, see [Oracle database log files \(p. 709\)](#).

Troubleshooting Oracle replication failure after adding or modifying triggers

If you add or modify any triggers, and if replication fails afterward, the problem may be the triggers. Ensure that the trigger excludes the following user accounts, which are required by RDS for replication:

- User accounts with administrator privileges
- SYS
- SYSTEM
- RDS_DATAGUARD

- `rdsdb`

For more information, see [Miscellaneous considerations for RDS for Oracle replicas \(p. 1633\)](#).

Adding options to Oracle DB instances

In Amazon RDS, an *option* is an additional feature. Following, you can find a description of options that you can add to Amazon RDS instances running the Oracle DB engine.

Topics

- [Overview of Oracle DB options \(p. 1646\)](#)
- [Amazon S3 integration \(p. 1648\)](#)
- [Oracle Application Express \(APEX\) \(p. 1664\)](#)
- [Amazon EFS integration \(p. 1675\)](#)
- [Oracle Java virtual machine \(p. 1685\)](#)
- [Oracle Enterprise Manager \(p. 1688\)](#)
- [Oracle Label Security \(p. 1703\)](#)
- [Oracle Locator \(p. 1706\)](#)
- [Oracle Multimedia \(p. 1709\)](#)
- [Oracle native network encryption \(p. 1711\)](#)
- [Oracle OLAP \(p. 1719\)](#)
- [Oracle Secure Sockets Layer \(p. 1722\)](#)
- [Oracle Spatial \(p. 1730\)](#)
- [Oracle SQLT \(p. 1733\)](#)
- [Oracle Statspack \(p. 1739\)](#)
- [Oracle time zone \(p. 1742\)](#)
- [Oracle time zone file autoupgrade \(p. 1746\)](#)
- [Oracle Transparent Data Encryption \(p. 1751\)](#)
- [Oracle UTL_MAIL \(p. 1753\)](#)
- [Oracle XML DB \(p. 1756\)](#)

Overview of Oracle DB options

To enable options for your Oracle database, add them to an option group, and then associate the option group with your DB instance. For more information, see [Working with option groups \(p. 273\)](#).

Topics

- [Summary of Oracle Database options \(p. 1646\)](#)
- [Options supported for different editions \(p. 1647\)](#)
- [Memory requirements for specific options \(p. 1647\)](#)

Summary of Oracle Database options

You can add the following options for Oracle DB instances.

Option	Option ID
Amazon S3 integration (p. 1648)	S3_INTEGRATION
Oracle Application Express (APEX) (p. 1664)	APEX
	APEX-DEV

Option	Option ID
Oracle Enterprise Manager (p. 1688)	OEM
	OEM_AGENT
Oracle Java virtual machine (p. 1685)	JVM
Oracle Label Security (p. 1703)	OLS
Oracle Locator (p. 1706)	LOCATOR
Oracle Multimedia (p. 1709)	MULTIMEDIA
Oracle native network encryption (p. 1711)	NATIVE_NETWORK_ENCRYPTION
Oracle OLAP (p. 1719)	OLAP
Oracle Secure Sockets Layer (p. 1722)	SSL
Oracle Spatial (p. 1730)	Spatial
Oracle SQLT (p. 1733)	SQLT
Oracle Statspack (p. 1739)	STATSPACK
Oracle time zone (p. 1742)	TIMEZONE
Oracle time zone file autoupgrade (p. 1746)	TIMEZONE_FILE_AUTOUPGRADE
Oracle Transparent Data Encryption (p. 1751)	TDE
Oracle UTL_MAIL (p. 1753)	UTL_MAIL
Oracle XML DB (p. 1756)	XMLDB

Options supported for different editions

RDS for Oracle prevents you from adding options to an edition if they aren't supported. To find out which RDS options are supported in different Oracle Database editions, use the command `aws rds describe-option-group-options`. The following example lists supported options for Oracle Database 19c Enterprise Edition.

```
aws rds describe-option-group-options \
--engine-name oracle-ee \
--major-engine-version 19
```

For more information, see [describe-option-group-options](#) in the *AWS CLI Command Reference*.

Memory requirements for specific options

Some options require additional memory to run on your DB instance. For example, Oracle Enterprise Manager Database Control uses about 300 MB of RAM. If you enable this option for a small DB instance, you might encounter performance problems due to memory constraints. You can adjust the Oracle parameters so that the database requires less RAM. Alternatively, you can scale up to a larger DB instance.

Amazon S3 integration

You can transfer files between your RDS for Oracle DB instance and an Amazon S3 bucket. You can use Amazon S3 integration with Oracle Database features such as Oracle Data Pump. For example, you can download Data Pump files from Amazon S3 to your RDS for Oracle DB instance. For more information, see [Importing data into Oracle on Amazon RDS \(p. 1615\)](#).

Note

Your DB instance and your Amazon S3 bucket must be in the same AWS Region.

Topics

- [Configuring IAM permissions for RDS for Oracle integration with Amazon S3 \(p. 1648\)](#)
- [Adding the Amazon S3 integration option \(p. 1656\)](#)
- [Transferring files between Amazon RDS for Oracle and an Amazon S3 bucket \(p. 1657\)](#)
- [Removing the Amazon S3 integration option \(p. 1663\)](#)

Configuring IAM permissions for RDS for Oracle integration with Amazon S3

For RDS for Oracle to integrate with Amazon S3, your DB instance must have access to an Amazon S3 bucket. The Amazon VPC used by your DB instance doesn't need to provide access to the Amazon S3 endpoints.

RDS for Oracle supports uploading files from a DB instance in one account to an Amazon S3 bucket in a different account. Where additional steps are required, they are noted in the following sections.

Topics

- [Step 1: Create an IAM policy for your Amazon RDS role \(p. 1648\)](#)
- [Step 2: \(Optional\) Create an IAM policy for your Amazon S3 bucket \(p. 1651\)](#)
- [Step 3: Create an IAM role for your DB instance and attach your policy \(p. 1653\)](#)
- [Step 4: Associate your IAM role with your RDS for Oracle DB instance \(p. 1655\)](#)

Step 1: Create an IAM policy for your Amazon RDS role

In this step, you create an AWS Identity and Access Management (IAM) policy with the permissions required to transfer files from your Amazon S3 bucket to your RDS DB instance.

To create the policy, make sure you have the following:

- The Amazon Resource Name (ARN) for your bucket
- The ARN for your AWS KMS key, if your bucket uses SSE-KMS or SSE-S3 encryption

Note

An Oracle DB instance can't access Amazon S3 buckets encrypted with SSE-C.

For more information, see [Protecting data using server-side encryption](#) in the *Amazon Simple Storage Service User Guide*.

Console

To create an IAM policy to allow Amazon RDS access to an Amazon S3 bucket

1. Open the [IAM Management Console](#).
2. Under **Access management**, choose **Policies**.

3. Choose **Create Policy**.
4. On the **Visual editor** tab, choose **Choose a service**, and then choose **S3**.
5. For **Actions**, choose **Expand all**, and then choose the bucket permissions and object permissions required to transfer files from an Amazon S3 bucket to Amazon RDS. For example, do the following:
 - Expand **List**, and then select **ListBucket**.
 - Expand **Read**, and then select **GetObject**.
 - Expand **Write**, and then select **PutObject** and **DeleteObject**.
 - Expand **Permissions management**, and then select **PutObjectAcl**. This permission is necessary if you plan to upload files to a bucket owned by a different account, and this account needs full control of the bucket contents.

Object permissions are permissions for object operations in Amazon S3. You must grant them for objects in a bucket, not the bucket itself. For more information, see [Permissions for object operations](#).

6. Choose **Resources**, and choose **Add ARN for bucket**.
7. In the **Add ARN(s)** dialog box, provide the details about your resource, and choose **Add**.

Specify the Amazon S3 bucket to allow access to. For instance, to allow Amazon RDS to access the Amazon S3 bucket named example-bucket, set the ARN value to `arn:aws:s3:::example-bucket`.

8. If the **object** resource is listed, choose **Add ARN for object**.
9. In the **Add ARN(s)** dialog box, provide the details about your resource.

For the Amazon S3 bucket, specify the Amazon S3 bucket to allow access to. For the object, you can choose **Any** to grant permissions to any object in the bucket.

Note

You can set **Amazon Resource Name (ARN)** to a more specific ARN value to allow Amazon RDS to access only specific files or folders in an Amazon S3 bucket. For more information about how to define an access policy for Amazon S3, see [Managing access permissions to your Amazon S3 resources](#).

10. (Optional) Choose **Add additional permissions** to add resources to the policy. For example, do the following:
 - If your bucket is encrypted with a custom KMS key, select **KMS** for the service. Select **Encrypt**, **ReEncrypt**, **Decrypt**, **DescribeKey**, and **GenerateDataKey** for actions. Enter the ARN of your custom key as the resource. For more information, see [Protecting Data Using Server-Side Encryption with KMS keys Stored in AWS Key Management Service \(SSE-KMS\)](#) in the *Amazon Simple Storage Service User Guide*.
 - If you want Amazon RDS to access to access other buckets, add the ARNs for these buckets. Optionally, you can also grant access to all buckets and objects in Amazon S3.
11. Choose **Next: Tags** and then **Next: Review**.
12. For **Name**, enter a name for your IAM policy, for example `rds-s3-integration-policy`. You use this name when you create an IAM role to associate with your DB instance. You can also add an optional **Description** value.
13. Choose **Create policy**.

AWS CLI

Create an AWS Identity and Access Management (IAM) policy that grants Amazon RDS access to an Amazon S3 bucket. After you create the policy, note the ARN of the policy. You need the ARN for a subsequent step.

Include the appropriate actions in the policy based on the type of access required:

- `GetObject` – Required to transfer files from an Amazon S3 bucket to Amazon RDS.
- `ListBucket` – Required to transfer files from an Amazon S3 bucket to Amazon RDS.
- `PutObject` – Required to transfer files from Amazon RDS to an Amazon S3 bucket.

The following AWS CLI command creates an IAM policy named `rds-s3-integration-policy` with these options. It grants access to a bucket named `your-s3-bucket-arn`.

Example

For Linux, macOS, or Unix:

```
aws iam create-policy \
--policy-name rds-s3-integration-policy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3integration",
            "Action": [
                "s3:GetObject",
                "s3>ListBucket",
                "s3:PutObject"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::your-s3-bucket-arn",
                "arn:aws:s3:::your-s3-bucket-arn/*"
            ]
        }
    ]
}'
```

The following example includes permissions for custom KMS keys.

```
aws iam create-policy \
--policy-name rds-s3-integration-policy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3integration",
            "Action": [
                "s3:GetObject",
                "s3>ListBucket",
                "s3:PutObject",
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:ReEncrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::your-s3-bucket-arn",
                "arn:aws:s3:::your-s3-bucket-arn/*",
                "arn:aws:kms:::your-kms-arn"
            ]
        }
    ]
}'
```

```
 }'
```

For Windows:

```
aws iam create-policy ^
--policy-name rds-s3-integration-policy ^
--policy-document '{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "s3integration",
      "Action": [
        "s3:GetObject",
        "s3>ListBucket",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::your-s3-bucket-arn",
        "arn:aws:s3:::your-s3-bucket-arn/*"
      ]
    }
  ]
}'
```

The following example includes permissions for custom KMS keys.

```
aws iam create-policy ^
--policy-name rds-s3-integration-policy ^
--policy-document '{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "s3integration",
      "Action": [
        "s3:GetObject",
        "s3>ListBucket",
        "s3:PutObject",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::your-s3-bucket-arn",
        "arn:aws:s3:::your-s3-bucket-arn/*",
        "arn:aws:kms:::your-kms-arn"
      ]
    }
  ]
}'
```

Step 2: (Optional) Create an IAM policy for your Amazon S3 bucket

This step is necessary only in the following conditions:

- You plan to upload files to an Amazon S3 bucket from one account (account A) and access them from a different account (account B).
- Account B owns the bucket.

- Account B needs full control of objects loaded into the bucket.

If the preceding conditions don't apply to you, skip to [Step 3: Create an IAM role for your DB instance and attach your policy \(p. 1653\)](#).

To create your bucket policy, make sure you have the following:

- The account ID for account A
- The user name for account A
- The ARN value for the Amazon S3 bucket in account B

Console

To create or edit a bucket policy

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to create a bucket policy for or whose bucket policy you want to edit.
3. Choose **Permissions**.
4. Under **Bucket policy**, choose **Edit**. This opens the Edit bucket policy page.
5. On the **Edit bucket policy** page, explore **Policy examples** in the *Amazon S3 User Guide*, choose **Policy generator** to generate a policy automatically, or edit the JSON in the **Policy** section.

If you choose **Policy generator**, the AWS Policy Generator opens in a new window:

- a. On the **AWS Policy Generator** page, in **Select Type of Policy**, choose **S3 Bucket Policy**.
- b. Add a statement by entering the information in the provided fields, and then choose **Add Statement**. Repeat for as many statements as you would like to add. For more information about these fields, see the [IAM JSON policy elements reference](#) in the *IAM User Guide*.

Note

For convenience, the **Edit bucket policy** page displays the **Bucket ARN** (Amazon Resource Name) of the current bucket above the **Policy** text field. You can copy this ARN for use in the statements on the **AWS Policy Generator** page.

- c. After you finish adding statements, choose **Generate Policy**.
 - d. Copy the generated policy text, choose **Close**, and return to the **Edit bucket policy** page in the Amazon S3 console.
6. In the **Policy** box, edit the existing policy or paste the bucket policy from the Policy generator. Make sure to resolve security warnings, errors, general warnings, and suggestions before you save your policy.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Example permissions",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::account-A-ID:account-A-user"  
            },  
            "Action": [  
                "s3:PutObject",  
                "s3:PutObjectAcl"  
            ],  
            "Resource": [  
                "arn:aws:s3:::mybucket/*"  
            ]  
        }  
    ]  
}
```

```
        "arn:aws:s3:::account-B-bucket-arn",  
        "arn:aws:s3:::account-B-bucket-arn/*"  
    ]  
}  
]
```

7. Choose **Save changes**, which returns you to the Bucket Permissions page.

Step 3: Create an IAM role for your DB instance and attach your policy

This step assumes that you have created the IAM policy in [Step 1: Create an IAM policy for your Amazon RDS role \(p. 1648\)](#). In this step, you create a role for your RDS for Oracle DB instance and then attach your policy to the role.

Console

To create an IAM role to allow Amazon RDS access to an Amazon S3 bucket

1. Open the [IAM Management Console](#).
2. In the navigation pane, choose **Roles**.
3. Choose **Create role**.
4. For **AWS service**, choose **RDS**.
5. For **Select your use case**, choose **RDS – Add Role to Database**.
6. Choose **Next**.
7. For **Search under Permissions policies**, enter the name of the IAM policy you created, and choose the policy when it appears in the list.
8. Choose **Next**.
9. Set **Role name** to a name for your IAM role, for example `rds-s3-integration-role`. You can also add an optional **Description** value.
10. Choose **Create role**.

AWS CLI

To create a role and attach your policy to it

1. Create an IAM role that Amazon RDS can assume on your behalf to access your Amazon S3 buckets.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based trust relationships to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the trust relationship, make sure to use the `aws:SourceArn` global condition context key with the full Amazon Resource Name (ARN) of the resources accessing the role.

The following AWS CLI command creates the role named `rds-s3-integration-role` for this purpose.

Example

For Linux, macOS, or Unix:

```
aws iam create-role \
--role-name rds-s3-integration-role \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": my_account_ID,
                    "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
                }
            }
        ]
}'
```

For Windows:

```
aws iam create-role ^
--role-name rds-s3-integration-role ^
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": my_account_ID,
                    "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
                }
            }
        ]
}'
```

For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

2. After the role is created, note the ARN of the role. You need the ARN for a subsequent step.
3. Attach the policy you created to the role you created.

The following AWS CLI command attaches the policy to the role named *rds-s3-integration-role*.

Example

For Linux, macOS, or Unix:

```
aws iam attach-role-policy \
--policy-arn your-policy-arn \
--role-name rds-s3-integration-role
```

For Windows:

```
aws iam attach-role-policy ^
--policy-arn your-policy-arn ^
--role-name rds-s3-integration-role
```

Replace *your-policy-arn* with the policy ARN that you noted in a previous step.

Step 4: Associate your IAM role with your RDS for Oracle DB instance

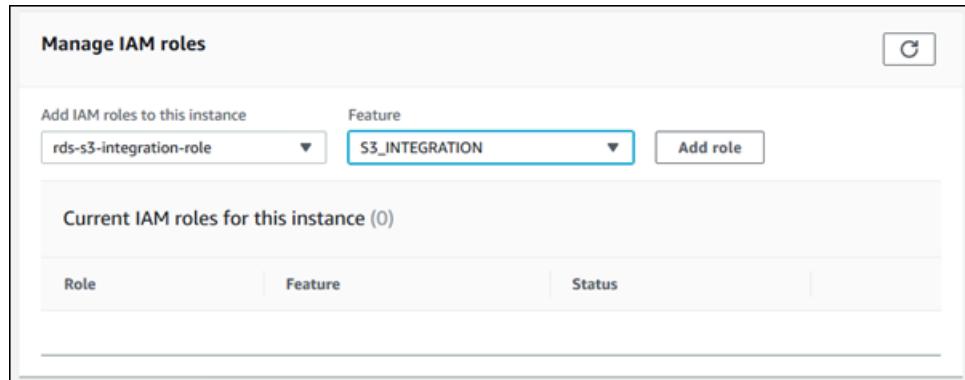
The last step in configuring permissions for Amazon S3 integration is associating your IAM role with your DB instance. Note the following requirements:

- You must have access to an IAM role with the required Amazon S3 permissions policy attached to it.
- You can only associate one IAM role with your RDS for Oracle at a time.
- The status of your instance must be available.

Console

To associate your IAM role with your RDS for Oracle DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Databases** from the navigation pane.
3. If your database instance is unavailable, choose **Actions** and then **Start**. When the instance status shows **Started**, go to the next step.
4. Choose the Oracle DB instance name to display its details.
5. On the **Connectivity & security** tab, scroll down to the **Manage IAM roles** section at the bottom of the page.
6. Choose the role to add in the **Add IAM roles to this instance** section.
7. For **Feature**, choose **S3_INTEGRATION**.



8. Choose **Add role**.

AWS CLI

The following AWS CLI command adds the role to an Oracle DB instance named *mydbinstance*.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-instance \
--db-instance-identifier mydbinstance \
--feature-name S3_INTEGRATION \
--role-arn your-role-arn
```

For Windows:

```
aws rds add-role-to-db-instance ^
--db-instance-identifier mydbinstance ^
--feature-name S3_INTEGRATION ^
--role-arn your-role-arn
```

Replace *your-role-arn* with the role ARN that you noted in a previous step. S3_INTEGRATION must be specified for the --feature-name option.

Adding the Amazon S3 integration option

To use Amazon RDS for Oracle Integration with Amazon S3, your Amazon RDS for Oracle DB instance must be associated with an option group that includes the S3_INTEGRATION option.

Console

To configure an option group for Amazon S3 integration

1. Create a new option group or identify an existing option group to which you can add the S3_INTEGRATION option.

For information about creating an option group, see [Creating an option group \(p. 274\)](#).

2. Add the S3_INTEGRATION option to the option group.

For information about adding an option to an option group, see [Adding an option to an option group \(p. 277\)](#).

3. Create a new Oracle DB instance and associate the option group with it, or modify an Oracle DB instance to associate the option group with it.

For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

For information about modifying an Oracle DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

To configure an option group for Amazon S3 integration

1. Create a new option group or identify an existing option group to which you can add the S3_INTEGRATION option.

For information about creating an option group, see [Creating an option group \(p. 274\)](#).

2. Add the S3_INTEGRATION option to the option group.

For example, the following AWS CLI command adds the S3_INTEGRATION option to an option group named **myoptiongroup**.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name myoptiongroup \
--options OptionName=S3_INTEGRATION,OptionVersion=1.0
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name myoptiongroup ^
--options OptionName=S3_INTEGRATION,OptionVersion=1.0
```

3. Create a new Oracle DB instance and associate the option group with it, or modify an Oracle DB instance to associate the option group with it.

For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

For information about modifying an Oracle DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Transferring files between Amazon RDS for Oracle and an Amazon S3 bucket

To transfer files between an Oracle DB instance and an Amazon S3 bucket, you can use the Amazon RDS package `rdsadmin_s3_tasks`. You can compress files with GZIP when uploading them, and decompress them when downloading.

Note

The procedures in `rdsadmin_s3_tasks` upload or download the files in a single directory. You can't include subdirectories in these operations.

Topics

- [Uploading files from your RDS for Oracle DB instance to an Amazon S3 bucket \(p. 1657\)](#)
- [Downloading files from an Amazon S3 bucket to an Oracle DB instance \(p. 1660\)](#)
- [Monitoring the status of a file transfer \(p. 1662\)](#)

Uploading files from your RDS for Oracle DB instance to an Amazon S3 bucket

To upload files from your DB instance to an Amazon S3 bucket, use the procedure `rdsadmin.rdsadmin_s3_tasks.upload_to_s3`. For example, you can upload Oracle Recovery Manager (RMAN) backup files or Oracle Data Pump files. The maximum object size in an Amazon S3 bucket is 5 TB. For more information about working with objects, see [Amazon Simple Storage Service User Guide](#). For more information about performing RMAN backups, see [Performing common RMAN tasks for Oracle DB instances \(p. 1568\)](#).

The `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_bucket_name	VARCHAR2	–	required	The name of the Amazon S3 bucket to upload files to.
p_directory_name	VARCHAR2	–	required	The name of the Oracle directory object to upload files from. The directory can be any user-created directory object or the Data Pump directory, such as DATA_PUMP_DIR. Note You can only upload files from the specified directory. You can't upload files in subdirectories in the specified directory.
p_s3_prefix	VARCHAR2	–	required	An Amazon S3 file name prefix that files are uploaded to. An empty prefix uploads all files to the top level in the specified Amazon S3 bucket and doesn't add a prefix to the file names. For example, if the prefix is folder_1/oradb, files are uploaded to folder_1. In this case, the oradb prefix is added to each file.
p_prefix	VARCHAR2	–	required	A file name prefix that file names must match to be uploaded. An empty prefix uploads all files in the specified directory.
p_compression_level	NUMBER	0	optional	The level of GZIP compression. Valid values range from 0 to 9: <ul style="list-style-type: none">• 0 – No compression• 1 – Fastest compression• 9 – Highest compression
p_bucket_owner_full_control	VARCHAR2	–	optional	The access control setting for the bucket. The only valid values are null or FULL_CONTROL. This setting is required only

Parameter name	Data type	Default	Required	Description
				if you upload files from one account (account A) into a bucket owned by a different account (account B), and account B needs full control of the files.

The return value for the `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` procedure is a task ID.

The following example uploads all of the files in the `DATA_PUMP_DIR` directory to the Amazon S3 bucket named `mys3bucket`. The files aren't compressed.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name    => 'mys3bucket',
    p_prefix         => '',
    p_s3_prefix      => '',
    p_directory_name => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

The following example uploads all of the files with the prefix `db` in the `DATA_PUMP_DIR` directory to the Amazon S3 bucket named `mys3bucket`. Amazon RDS applies the highest level of GZIP compression to the files.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name    => 'mys3bucket',
    p_prefix         => 'db',
    p_s3_prefix      => '',
    p_directory_name => 'DATA_PUMP_DIR',
    p_compression_level => 9)
AS TASK_ID FROM DUAL;
```

The following example uploads all of the files in the `DATA_PUMP_DIR` directory to the Amazon S3 bucket named `mys3bucket`. The files are uploaded to a `dbfiles` folder. In this example, the GZIP compression level is `1`, which is the fastest level of compression.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name    => 'mys3bucket',
    p_prefix         => '',
    p_s3_prefix      => 'dbfiles/',
    p_directory_name => 'DATA_PUMP_DIR',
    p_compression_level => 1)
AS TASK_ID FROM DUAL;
```

The following example uploads all of the files in the `DATA_PUMP_DIR` directory to the Amazon S3 bucket named `mys3bucket`. The files are uploaded to a `dbfiles` folder and `ora` is added to the beginning of each file name. No compression is applied.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name    => 'mys3bucket',
    p_prefix         => '',
    p_s3_prefix      => 'dbfiles/ora',
    p_directory_name => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

The following example assumes that the command is run in account A, but account B requires full control of the bucket contents. The command `rdsadmin_s3_tasks.upload_to_s3` transfers all files in the

`DATA_PUMP_DIR` directory to the bucket named `s3bucketOwnedByAccountB`. Access control is set to FULL_CONTROL so that account B can access the files in the bucket. The GZIP compression level is 6, which balances speed and file size.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
    p_bucket_name          => 's3bucketOwnedByAccountB',
    p_prefix                => '',
    p_s3_prefix              => '',
    p_directory_name        => 'DATA_PUMP_DIR',
    p_bucket_owner_full_control => 'FULL_CONTROL',
    p_compression_level      => 6)
AS TASK_ID FROM DUAL;
```

In each example, the SELECT statement returns the ID of the task in a VARCHAR2 data type.

You can view the result by displaying the task's output file.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP', 'dbtask-task-id.log'));
```

Replace `task-id` with the task ID returned by the procedure.

Note

Tasks are executed asynchronously.

Downloading files from an Amazon S3 bucket to an Oracle DB instance

To download files from an Amazon S3 bucket to an RDS for Oracle instance, use the Amazon RDS procedure `rdsadmin.rdsadmin_s3_tasks.download_from_s3`.

When you download files using the procedure `download_from_s3`, consider the following:

- The download limit is 2000 files per procedure call. If you need to download more than 2000 files from Amazon S3, split your download into separate actions, with no more than 2000 files per procedure call.
- If a file exists in your download folder, and you attempt to download a file with the same name, `download_from_s3` skips the download. To remove a file from the download directory, use [UTL_FILE.FREMOVE](#), found on the Oracle website.

The `download_from_s3` procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_bucket_name	VARCHAR2 –		Required	The name of the Amazon S3 bucket to download files from.
p_directory_name	VARCHAR2 –		Required	The name of the Oracle directory object to download files to. The directory can be any user-created directory object or the Data Pump directory, such as DATA_PUMP_DIR.
p_error_on_zero_download	VARCHAR2 FALSE		Optional	A flag that determines whether the task raises an error when no objects in the Amazon S3 bucket match the prefix. If this parameter is not set or set to FALSE

Parameter name	Data type	Default	Required	Description
				<p>(default), the task prints a message that no objects were found, but doesn't raise an exception or fail. If this parameter is TRUE, the task raises an exception and fails.</p> <p>Examples of prefix specifications that can fail match tests are spaces in prefixes, as in ' import/test9.log ', and case mismatches, as in test9.log and test9.LOG.</p>
p_s3_prefix	VARCHAR2 –		Required	<p>A file name prefix that file names must match to be downloaded. An empty prefix downloads all of the top level files in the specified Amazon S3 bucket, but not the files in folders in the bucket.</p> <p>The procedure downloads Amazon S3 objects only from the first level folder that matches the prefix. Nested directory structures matching the specified prefix are not downloaded.</p> <p>For example, suppose that an Amazon S3 bucket has the folder structure folder_1/folder_2/folder_3. You specify the 'folder_1/folder_2/' prefix. In this case, only the files in folder_2 are downloaded, not the files in folder_1 or folder_3.</p> <p>If, instead, you specify the 'folder_1/folder_2' prefix, all files in folder_1 that match the 'folder_2' prefix are downloaded, and no files in folder_2 are downloaded.</p>
p_decompression_format	VARCHAR2 –		Optional	The decompression format. Valid values are NONE for no decompression and GZIP for decompression.

The return value for the `rdsadmin.rdsadmin_s3_tasks.download_from_s3` procedure is a task ID.

The following example downloads all files in the Amazon S3 bucket named `mys3bucket` to the `DATA_PUMP_DIR` directory. The files aren't compressed, so no decompression is applied.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name => 'mys3bucket',
    p_directory_name => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

The following example downloads all of the files with the prefix `db` in the Amazon S3 bucket named `mys3bucket` to the `DATA_PUMP_DIR` directory. The files are compressed with GZIP, so decompression is

applied. The parameter `p_error_on_zero_downloads` turns on prefix error checking, so if the prefix doesn't match any files in the bucket, the task raises an exception and fails.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name      => 'mys3bucket',
    p_s3_prefix        => 'db',
    p_directory_name   => 'DATA_PUMP_DIR',
    p_decompression_format => 'GZIP',
    p_error_on_zero_downloads => 'TRUE')
AS TASK_ID FROM DUAL;
```

The following example downloads all of the files in the folder `myfolder/` in the Amazon S3 bucket named `mys3bucket` to the `DATA_PUMP_DIR` directory. Use the `p_s3_prefix` parameter to specify the Amazon S3 folder. The uploaded files are compressed with GZIP, but aren't decompressed during the download.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name      => 'mys3bucket',
    p_s3_prefix        => 'myfolder/',
    p_directory_name   => 'DATA_PUMP_DIR',
    p_decompression_format => 'NONE')
AS TASK_ID FROM DUAL;
```

The following example downloads the file `mydumpfile.dmp` in the Amazon S3 bucket named `mys3bucket` to the `DATA_PUMP_DIR` directory. No decompression is applied.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
    p_bucket_name      => 'mys3bucket',
    p_s3_prefix        => 'mydumpfile.dmp',
    p_directory_name   => 'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

In each example, the SELECT statement returns the ID of the task in a VARCHAR2 data type.

You can view the result by displaying the task's output file.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP', 'dbtask-task-id.log'));
```

Replace `task-id` with the task ID returned by the procedure.

Note

Tasks are executed asynchronously.

You can use the `UTL_FILE.FREMOVE` Oracle procedure to remove files from a directory. For more information, see [FREMOVE procedure](#) in the Oracle documentation.

Monitoring the status of a file transfer

File transfer tasks publish Amazon RDS events when they start and when they complete. For information about viewing events, see [Viewing Amazon RDS events \(p. 647\)](#).

You can view the status of an ongoing task in a bdump file. The bdump files are located in the `/rdsdbdata/log/trace` directory. Each bdump file name is in the following format.

```
dbtask-task-id.log
```

Replace `task-id` with the ID of the task that you want to monitor.

Note

Tasks are executed asynchronously.

You can use the `rdsadmin.rds_file_util.read_text_file` stored procedure to view the contents of bdump files. For example, the following query returns the contents of the `dbtask-1546988886389-2444.log` bdump file.

```
SELECT text FROM
  table(rdsadmin.rds_file_util.read_text_file('BDUMP', 'dbtask-1546988886389-2444.log'));
```

Removing the Amazon S3 integration option

You can remove Amazon S3 integration option from a DB instance.

To remove the Amazon S3 integration option from a DB instance, do one of the following:

- To remove the Amazon S3 integration option from multiple DB instances, remove the `S3_INTEGRATION` option from the option group to which the DB instances belong. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove the Amazon S3 integration option from a single DB instance, modify the instance and specify a different option group that doesn't include the `S3_INTEGRATION` option. You can specify the default (empty) option group or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Application Express (APEX)

Amazon RDS supports Oracle Application Express (APEX) through the use of the APEX and APEX-DEV options. Oracle APEX can be deployed as a run-time environment or as a full development environment for web-based applications. Using Oracle APEX, developers can build applications entirely within the web browser. For more information, see [Oracle application Express](#) in the Oracle documentation.

Topics

- [APEX components \(p. 1664\)](#)
- [APEX version requirements \(p. 1664\)](#)
- [Prerequisites for Oracle APEX and ORDS \(p. 1665\)](#)
- [Adding the Amazon RDS APEX options \(p. 1666\)](#)
- [Unlocking the public user account \(p. 1666\)](#)
- [Configuring RESTful services for Oracle APEX \(p. 1667\)](#)
- [Setting up ORDS for Oracle APEX \(p. 1667\)](#)
- [Setting up Oracle APEX listener \(p. 1671\)](#)
- [Upgrading the APEX version \(p. 1673\)](#)
- [Removing the APEX option \(p. 1673\)](#)

APEX components

Oracle APEX consists of the following main components:

- A *repository* that stores the metadata for APEX applications and components. The repository consists of tables, indexes, and other objects that are installed in your Amazon RDS DB instance.
- A *listener* that manages HTTP communications with Oracle APEX clients. The listener accepts incoming connections from web browsers, forwards them to the Amazon RDS DB instance for processing, and then sends results from the repository back to the browsers. Amazon RDS for Oracle supports the following types of listeners:
 - For APEX version 5.0 and later, use Oracle Rest Data Services (ORDS) version 19.1 and higher. We recommend that you use the latest supported version of Oracle APEX and ORDS. This documentation describes older versions for backwards compatibility only.
 - For APEX version 4.1.1, you can use Oracle APEX Listener version 1.1.4.
 - You can use Oracle HTTP Server and mod_plsql listeners.

Note

Amazon RDS doesn't support the Oracle XML DB HTTP server with the embedded PL/SQL gateway; you can't use this as a listener for APEX. In general, Oracle recommends against using the embedded PL/SQL gateway for applications that run on the internet.

For more information about these listener types, see [About choosing a web listener](#) in the Oracle documentation.

When you add the Amazon RDS APEX options to your DB instance, Amazon RDS installs the Oracle APEX repository only. Install your listener on a separate host, such as an Amazon EC2 instance, an on-premises server at your company, or your desktop computer.

APEX version requirements

The APEX option uses storage on the DB instance class for your DB instance. Following are the supported versions and approximate storage requirements for Oracle APEX.

APEX version	Storage requirements	Supported Oracle Database versions	Notes
Oracle APEX version 22.1.v1	124 MiB	All	This version includes patch 34020981: PSE BUNDLE FOR APEX 22.1 (PSSES ON TOP OF 22.1.0), PATCH_VERSION 6.
Oracle APEX version 21.2.v1	125 MiB	All	This version includes patch 33420059: PSE BUNDLE FOR APEX 21.2 (PSSES ON TOP OF 21.2.0), PATCH_VERSION 8.
Oracle APEX version 21.1.v1	125 MiB	All	This version includes patch 32598392: PSE BUNDLE FOR APEX 21.1, PATCH_VERSION 3.
Oracle APEX version 20.2.v1	148 MiB	All except 21c	<p>This version includes patch 32006852: PSE BUNDLE FOR APEX 20.2, PATCH_VERSION 2020.11.12. You can see the patch number and date by running the following query:</p> <pre>SELECT PATCH_VERSION, PATCH_NUMBER FROM APEX_PATCHES;</pre>
Oracle APEX version 20.1.v1	173 MiB	All except 21c	This version includes patch 30990551: PSE BUNDLE FOR APEX 20.1, PATCH_VERSION 2020.07.15.
Oracle APEX version 19.2.v1	149 MiB	All except 21c	
Oracle APEX version 19.1.v1	148 MiB	All except 21c	
Oracle APEX version 18.2.v1	146 MiB	12.1 and 12.2 only	
Oracle APEX version 18.1.v1	145 MiB	12.1 and 12.2 only	
Oracle APEX version 5.1.4.v1	220 MiB	12.1 and 12.2 only	
Oracle APEX version 5.1.2.v1	150 MiB	12.1 and 12.2 only	
Oracle APEX version 5.0.4.v1	140 MiB	12.1 and 12.2 only	
Oracle APEX version 4.2.6.v1	160 MiB	12.1 only	

Prerequisites for Oracle APEX and ORDS

To use Oracle APEX and ORDS, make sure you have the following:

- The Java Runtime Environment (JRE)
- An Oracle client installation that includes the following:

- SQL*Plus or SQL Developer for administration tasks
- Oracle Net Services for configuring connections to your Oracle instance

Adding the Amazon RDS APEX options

To add the Amazon RDS APEX options to a DB instance, do the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the options to the option group.
3. Associate the option group with the DB instance.

When you add the Amazon RDS APEX options, a brief outage occurs while your DB instance is automatically restarted.

To add the APEX options to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose the Oracle edition that you want to use. The APEX options are supported on all editions.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the options to the option group. If you want to deploy only the Oracle APEX run-time environment, add only the APEX option. If you want to deploy the full development environment, add both the APEX and APEX-DEV options. For Oracle Database 12c, add the **APEX** and **APEX-DEV** options.

For **Version**, choose the version of APEX that you want to use. If you don't choose a version, version 4.2.6.v1 is the default for Oracle Database 12c.

Important

If you add the APEX options to an existing option group that is already attached to one or more DB instances, a brief outage occurs. During this outage, all the DB instances are automatically restarted.

For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).

3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. When you add the APEX options to an existing DB instance, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Unlocking the public user account

After the Amazon RDS APEX options are installed, make sure to do the following:

1. Change the password for the APEX public user account.

2. Unlock the account.

You can do this by using the Oracle SQL*Plus command line utility. Connect to your DB instance as the master user, and issue the following commands. Replace `new_password` with a password of your choice.

```
ALTER USER APEX_PUBLIC_USER IDENTIFIED BY new_password;
ALTER USER APEX_PUBLIC_USER ACCOUNT UNLOCK;
```

Configuring RESTful services for Oracle APEX

To configure RESTful services in APEX (not needed for APEX 4.1.1.V1), use SQL*Plus to connect to your DB instance as the master user. After you do this, run the `rdsadmin.rdsadmin_run_apex_rest_config` stored procedure. When you run the stored procedure, you provide passwords for the following users:

- `APEX_LISTENER`
- `APEX_REST_PUBLIC_USER`

The stored procedure runs the `apex_rest_config.sql` script, which creates new database accounts for these users.

Note

Configuration isn't required for Oracle APEX version 4.1.1.v1. For this Oracle APEX version only, you don't need to run the stored procedure.

The following command runs the stored procedure.

```
EXEC rdsadmin.rdsadmin_run_apex_rest_config('apex_listener_password',
                                              'apex_rest_public_user_password');
```

Setting up ORDS for Oracle APEX

You are now ready to install and configure Oracle Rest Data Services (ORDS) for use with Oracle APEX. For APEX version 5.0 and later, use Oracle Rest Data Services (ORDS) version 19.1 and higher.

Install the listener on a separate host such as an Amazon EC2 instance, an on-premises server at your company, or your desktop computer. For the examples in this section, we assume that the name of your host is `myapexhost.example.com`, and that your host is running Linux.

Preparing to install ORDS

Before you can install ORDS, you need to create a nonprivileged OS user, and then download and unzip the APEX installation file.

To prepare for ORDS installation

1. Log in to `myapexhost.example.com` as `root`.
2. Create a nonprivileged OS user to own the listener installation. The following command creates a new user named `apexuser`.

```
useradd -d /home/apexuser apexuser
```

The following command assigns a password to the new user.

```
passwd apexuser;
```

3. Log in to myapexhost.example.com as apexuser, and download the APEX installation file from Oracle to your /home/apexuser directory:
 - <http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html>
 - [Oracle application Express prior release archives](#)
4. Unzip the file in the /home/apexuser directory.

```
unzip apex_<version>.zip
```

After you unzip the file, there is an apex directory in the /home/apexuser directory.

5. While you are still logged into myapexhost.example.com as apexuser, download the Oracle REST Data Services file from Oracle to your /home/apexuser directory: <http://www.oracle.com/technetwork/developer-tools/apex-listener/downloads/index.html>.

Installing and configuring ORDS

Before you can use APEX, you need to download the ords.war file, use Java to install ORDS, and then start the listener.

To install and configure ORDS for use with Oracle APEX

1. Create a new directory based on ORDS, and then unzip the listener file.

```
mkdir /home/apexuser/ORDS
cd /home/apexuser/ORDS
```

2. Download the file ords.*version.number*.zip from [Oracle REST data services](#).
3. Unzip the file into the /home/apexuser/ORDS directory.
4. If you're installing ORDS in a multitenant database, add the following line to the file /home/apexuser/ORDS/params/ords_params.properties:

```
pdb.disable.lockdown=false
```

5. Grant the master user the required privileges to install ORDS.

After the Amazon RDS APEX option is installed, give the master user the required privileges to install the ORDS schema. You can do this by connecting to the database and running the following commands. Replace **MASTER_USER** with the uppercase name of your master user.

Important

When you enter the user name, use uppercase unless you created the user with a case-sensitive identifier. For example, if you run CREATE USER myuser or CREATE USER MYUSER, the data dictionary stores MYUSER. However, if you use double quotes in CREATE USER "MyUser", the data dictionary stores MyUser. For more information, see [Granting SELECT or EXECUTE privileges to SYS objects \(p. 1533\)](#).

```
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_OBJECTS', 'MASTER_USER', 'SELECT',
    true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_ROLE_PRIVS', 'MASTER_USER', 'SELECT',
    true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_COLUMNS', 'MASTER_USER',
    'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONS_COLUMNS', 'MASTER_USER',
    'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONSTRAINTS', 'MASTER_USER',
    'SELECT', true);
```

```
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_OBJECTS', 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER PROCEDURES', 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TAB_COLUMNS', 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TABLES', 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_VIEWS', 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('WPIUTL', 'MASTER_USER', 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_SESSION', 'MASTER_USER', 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS UTILITY', 'MASTER_USER', 'EXECUTE', true);
```

Note

These commands apply to ORDS version 19.1 and later.

6. Install the ORDS schema using the downloaded ords.war file.

```
java -jar ords.war install advanced
```

The program prompts you for the following information. The default values are in brackets. For more information, see [Introduction to Oracle REST data services](#) in the Oracle documentation.

- Enter the location to store configuration data:

Enter `/home/apexuser/ORDS`. This is the location of the ORDS configuration files.

- Specify the database connection type to use. Enter number for [1] Basic [2] TNS [3] Custom URL [1]:

Choose the desired connection type.

- Enter the name of the database server [localhost]: `DB_instance_endpoint`

Choose the default or enter the correct value.

- Enter the database listener port [1521]: `DB_instance_port`

Choose the default or enter the correct value.

- Enter 1 to specify the database service name, or 2 to specify the database SID [1]:

Choose 2 to specify the database SID.

- Database SID [xe]

Choose the default or enter the correct value.

- Enter 1 if you want to verify/install Oracle REST Data Services schema or 2 to skip this step [1]:

Choose 1. This step creates the Oracle REST Data Services proxy user named ORDS_PUBLIC_USER.

- Enter the database password for ORDS_PUBLIC_USER:

Enter the password, and then confirm it.

- Requires to login with administrator privileges to verify Oracle REST Data Services schema.

Enter the administrator user name: `master_user`

Enter the database password for `master_user`: `master_user_password`

Confirm the password: `master_user_password`

- Enter the default tablespace for ORDS_METADATA [SYSAUX].
Enter the temporary tablespace for ORDS_METADATA [TEMP].
Enter the default tablespace for ORDS_PUBLIC_USER [USERS].
Enter the temporary tablespace for ORDS_PUBLIC_USER [TEMP].
 - Enter 1 if you want to use PL/SQL Gateway or 2 to skip this step. If you're using Oracle Application Express or migrating from mod_plsql, you must enter 1 [1].
Choose the default.
 - Enter the PL/SQL Gateway database user name [APEX_PUBLIC_USER]
 - Choose the default.
 - Enter the database password for APEX_PUBLIC_USER:
Enter the password, and then confirm it.
 - Enter 1 to specify passwords for Application Express RESTful Services database users (APEX_LISTENER, APEX_REST_PUBLIC_USER) or 2 to skip this step [1]:
Choose 2 for APEX 4.1.1.V1; choose 1 for all other APEX versions.
 - [Not needed for APEX 4.1.1.v1] Database password for APEX_LISTENER
Enter the password (if required), and then confirm it.
 - [Not needed for APEX 4.1.1.v1] Database password for APEX_REST_PUBLIC_USER
Enter the password (if required), and then confirm it.
 - Enter a number to select a feature to enable:
Enter 1 to enable all features: SQL Developer Web, REST Enabled SQL, and Database API.
 - Enter 1 if you wish to start in standalone mode or 2 to exit [1]:
Enter 1.
 - Enter the APEX static resources location:
If you unzipped APEX installation files into /home/apexuser, enter /home/apexuser/apex/images. Otherwise, enter *unzip_path*/apex/images, where *unzip_path* is the directory where you unzipped the file.
 - Enter 1 if using HTTP or 2 if using HTTPS [1]:
If you enter 1, specify the HTTP port. If you enter 2, specify the HTTPS port and the SSL host name. The HTTPS option prompts you to specify how you will provide the certificate:
 - Enter 1 to use the self-signed certificate.
 - Enter 2 to provide your own certificate. If you enter 2, specify the path for the SSL certificate and the path for the SSL certificate private key.
7. Set a password for the APEX admin user. To do this, use SQL*Plus to connect to your DB instance as the master user, and then run the following commands.

```
EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
grant APEX_ADMINISTRATOR_ROLE to master;
@/home/apexuser/apex/apxchpwd.sql
```

Replace *master* with your master user name. When the apxchpwd.sql script prompts you, enter a new admin password.

8. Start the ORDS listener. Run the following code.

```
java -jar ords.war
```

The first time you start ORDS, you are prompted to provide the location of the APEX Static resources. This images folder is located in the /apex/images directory in the installation directory for APEX.

9. Return to the APEX administration window in your browser and choose **Administration**. Next, choose **Application Express Internal Administration**. When you are prompted for credentials, enter the following information:

- **User name** – admin
- **Password** – the password you set using the apxchpwd.sql script

Choose **Login**, and then set a new password for the admin user.

Your listener is now ready for use.

Setting up Oracle APEX listener

Note

Oracle APEX Listener is deprecated.

Amazon RDS for Oracle continues to support APEX version 4.1.1 and Oracle APEX Listener version 1.1.4. We recommend that you use the latest supported versions of Oracle APEX and ORDS.

Install Oracle APEX Listener on a separate host such as an Amazon EC2 instance, an on-premises server at your company, or your desktop computer. We assume that the name of your host is myapexhost.example.com, and that your host is running Linux.

Preparing to install Oracle APEX listener

Before you can install Oracle APEX Listener, you need to create a nonprivileged OS user, and then download and unzip the APEX installation file.

To prepare for Oracle APEX listener installation

1. Log in to myapexhost.example.com as root.
2. Create a nonprivileged OS user to own the listener installation. The following command creates a new user named *apexuser*.

```
useradd -d /home/apexuser apexuser
```

The following command assigns a password to the new user.

```
passwd apexuser;
```

3. Log in to myapexhost.example.com as apexuser, and download the APEX installation file from Oracle to your /home/apexuser directory:
 - <http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html>
 - [Oracle application Express prior release archives](#)
4. Unzip the file in the /home/apexuser directory.

```
unzip apex_<version>.zip
```

- After you unzip the file, there is an apex directory in the /home/apexuser directory.
5. While you are still logged into myapexhost.example.com as apexuser, download the Oracle APEX Listener file from Oracle to your /home/apexuser directory.

Installing and configuring Oracle APEX listener

Before you can use APEX, you need to download the apex.war file, use Java to install Oracle APEX Listener, and then start the listener.

To install and configure Oracle APEX listener

1. Create a new directory based on Oracle APEX Listener and open the listener file.

Run the following code:

```
mkdir /home/apexuser/apexlistener
cd /home/apexuser/apexlistener
unzip ../apex_listener.version.zip
```

2. Run the following code.

```
java -Dapex.home=../apex -Dapex.images=/home/apexuser/apex/images -Dapex.erase -jar ./apex.war
```

3. Enter information for the program prompts following:

- The APEX Listener Administrator user name. The default is *adminlistener*.
- A password for the APEX Listener Administrator.
- The APEX Listener Manager user name. The default is *managerlistener*.
- A password for the APEX Listener Administrator.

The program prints a URL that you need to complete the configuration, as follows.

```
INFO: Please complete configuration at: http://localhost:8080/apex/listenerConfigure
Database is not yet configured
```

4. Leave Oracle APEX Listener running so that you can use Oracle Application Express. When you have finished this configuration procedure, you can run the listener in the background.
5. From your web browser, go to the URL provided by the APEX Listener program. The Oracle Application Express Listener administration window appears. Enter the following information:
 - **Username** – APEX_PUBLIC_USER
 - **Password** – the password for APEX_PUBLIC_USER. This password is the one that you specified earlier when you configured the APEX repository. For more information, see [Unlocking the public user account \(p. 1666\)](#).
 - **Connection type** – Basic
 - **Hostname** – the endpoint of your Amazon RDS DB instance, such as mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com.
 - **Port** – 1521
 - **SID** – the name of the database on your Amazon RDS DB instance, such as mydb.
6. Choose **Apply**. The APEX administration window appears.
7. Set a password for the APEX admin user. To do this, use SQL*Plus to connect to your DB instance as the master user, and then run the following commands.

```
EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
grant APEX_ADMINISTRATOR_ROLE to master;
@/home/apexuser/apex/apxchpwd.sql
```

Replace *master* with your master user name. When the apxchpwd.sql script prompts you, enter a new admin password.

8. Return to the APEX administration window in your browser and choose **Administration**. Next, choose **Application Express Internal Administration**. When you are prompted for credentials, enter the following information:

- **User name** – admin
- **Password** – the password you set using the apxchpwd.sql script

Choose **Login**, and then set a new password for the admin user.

Your listener is now ready for use.

Upgrading the APEX version

Important

Back up your DB instance before you upgrade APEX. For more information, see [Creating a DB snapshot \(p. 448\)](#) and [Testing an Oracle DB upgrade \(p. 1763\)](#).

To upgrade APEX with your DB instance, do the following:

- Create a new option group for the upgraded version of your DB instance.
- Add the upgraded versions of APEX and APEX-DEV to the new option group. Be sure to include any other options that your DB instance uses. For more information, see [Option group considerations \(p. 1761\)](#).
- When you upgrade your DB instance, specify the new option group for your upgraded DB instance.

After you upgrade your version of APEX, the APEX schema for the previous version might still exist in your database. If you don't need it anymore, you can drop the old APEX schema from your database after you upgrade.

If you upgrade the APEX version and RESTful services were not configured in the previous APEX version, we recommend that you configure RESTful services. For more information, see [Configuring RESTful services for Oracle APEX \(p. 1667\)](#).

In some cases when you plan to do a major version upgrade of your DB instance, you might find that you're using an APEX version that isn't compatible with your target database version. In these cases, you can upgrade your version of APEX before you upgrade your DB instance. Upgrading APEX first can reduce the amount of time that it takes to upgrade your DB instance.

Note

After upgrading APEX, install and configure a listener for use with the upgraded version. For instructions, see [Setting up Oracle APEX listener \(p. 1671\)](#).

Removing the APEX option

You can remove the Amazon RDS APEX options from a DB instance. To remove the APEX options from a DB instance, do one of the following:

- To remove the APEX options from multiple DB instances, remove the APEX options from the option group they belong to. This change affects all DB instances that use the option group. When you

remove the APEX options from an option group that is attached to multiple DB instances, a brief outage occurs while all the DB instances are restarted.

For more information, see [Removing an option from an option group \(p. 285\)](#).

- To remove the APEX options from a single DB instance, modify the DB instance and specify a different option group that doesn't include the APEX options. You can specify the default (empty) option group, or a different custom option group. When you remove the APEX options, a brief outage occurs while your DB instance is automatically restarted.

For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

When you remove the APEX options from a DB instance, the APEX schema is removed from your database.

Amazon EFS integration

You can transfer files between your RDS for Oracle DB instance and an Amazon EFS file system. You can use Amazon EFS integration with Oracle Database features such as Oracle Data Pump. For example, you can import Data Pump files from Amazon EFS to your RDS for Oracle DB instance. You don't need to copy these files locally because Data Pump imports directly from the EFS file system. For more information, see [Importing data into Oracle on Amazon RDS \(p. 1615\)](#).

Note the following requirements and restrictions:

- Amazon EFS integration is supported only for Oracle Database 19c - July 2022 Patch Set Update (PSU) 19.0.0.0.ru-2022-07.rur-2022-07.r1 or later.
- Your DB instance and your EFS file system must be in the same AWS Region and the same VPC.
- Your VPC must have the `enableDnsSupport` attribute enabled. For more information, see [DNS attributes in your VPC](#) in the *Amazon Virtual Private Cloud User Guide*.
- Your EFS file system must use the Standard or Standard-IA storage class.
- RDS for Oracle doesn't support automated backups or manual DB snapshots of an EFS file system. Instead, you must use AWS Backup or other solutions to back up your EFS file system. For more information, see [Backing up your Amazon EFS file systems](#).

Topics

- [Configuring network permissions for RDS for Oracle integration with Amazon EFS \(p. 1675\)](#)
- [Configuring IAM permissions for RDS for Oracle integration with Amazon EFS \(p. 1676\)](#)
- [Adding the EFS_INTEGRATION option \(p. 1679\)](#)
- [Configuring Amazon EFS file system permissions \(p. 1680\)](#)
- [Transferring files between RDS for Oracle and an Amazon EFS file system \(p. 1681\)](#)
- [Removing the EFS_INTEGRATION option \(p. 1682\)](#)
- [Troubleshooting Amazon EFS integration \(p. 1682\)](#)

Configuring network permissions for RDS for Oracle integration with Amazon EFS

For RDS for Oracle to integrate with Amazon EFS, make sure that your DB instance has network access to an EFS file system. For more information, see [Controlling network access to Amazon EFS file systems for NFS clients](#) in the *Amazon Elastic File System User Guide*.

Topics

- [Controlling network access with security groups \(p. 1675\)](#)
- [Controlling network access with file system policies \(p. 1676\)](#)

Controlling network access with security groups

You can control your DB instance access to EFS file systems using network layer security mechanisms such as VPC security groups. To allow access to an EFS file system for your DB instance, make sure that your EFS file system meets the following requirements:

- A mount target exists in every Availability Zone.
- A security group is attached to the mount target.
- The security group has an inbound rule to allow the network subnet or security group of the RDS for Oracle DB instance on TCP/2049 (Type NFS).

For more information, see [Creating Amazon EFS file systems](#) and [Creating and managing EFS mount targets and security groups](#) in the *Amazon Elastic File System User Guide*.

Controlling network access with file system policies

Amazon EFS integration with RDS for Oracle works with the default (empty) EFS file system policy. The default policy doesn't use IAM to authenticate. Instead, it grants full access to any anonymous client that can connect to the file system using a mount target. The default policy is in effect whenever a user-configured file system policy isn't in effect, including at file system creation. For more information, see [Default EFS file system policy](#) in the *Amazon Elastic File System User Guide*.

To strengthen access to your EFS file system for all clients, including RDS for Oracle, you can configure IAM permissions. In this approach, you create a file system policy. For more information, see [Creating file system policies](#) in the *Amazon Elastic File System User Guide*.

Configuring IAM permissions for RDS for Oracle integration with Amazon EFS

For RDS for Oracle to integrate with Amazon EFS, your DB instance must have IAM permissions to access to an Amazon EFS file system.

Step 1: Create an IAM role for your DB instance and attach your policy

In this step, you create a role for your RDS for Oracle DB instance to allow Amazon RDS to access your EFS file system.

Console

To create an IAM role to allow Amazon RDS access to an EFS file system

1. Open the [IAM Management Console](#).
2. In the navigation pane, choose **Roles**.
3. Choose **Create role**.
4. For **AWS service**, choose **RDS**.
5. For **Select your use case**, choose **RDS – Add Role to Database**.
6. Choose **Next**.
7. Don't add any permissions policies. Choose **Next**.
8. Set **Role name** to a name for your IAM role, for example `rds-efs-integration-role`. You can also add an optional **Description** value.
9. Choose **Create role**.

AWS CLI

To limit the service's permissions to a specific resource, we recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based trust relationships. This is the most effective way to protect against the [confused deputy problem](#).

You might use both global condition context keys and have the `aws:SourceArn` value contain the account ID. In this case, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.

- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the trust relationship, make sure to use the `aws:SourceArn` global condition context key with the full Amazon Resource Name (ARN) of the resources accessing the role.

The following AWS CLI command creates the role named `rds-efs-integration-role` for this purpose.

Example

For Linux, macOS, or Unix:

```
aws iam create-role \
--role-name rds-efs-integration-role \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": my_account_ID,
                    "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
                }
            }
        ]
}'
```

For Windows:

```
aws iam create-role ^
--role-name rds-efs-integration-role ^
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": my_account_ID,
                    "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
                }
            }
        ]
}'
```

For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

Step 2: Create a file system policy for your Amazon EFS file system

In this step, you create a file system policy for your EFS file system.

To create or edit an EFS file system policy

1. Open the [EFS Management Console](#).
2. Choose **File Systems**.
3. On the **File systems** page, choose the file system that you want to edit or create a file system policy for. The details page for that file system is displayed.
4. Choose the **File system policy** tab.

If the policy is empty, then the default EFS file system policy is in use. For more information, see [Default EFS file system policy](#) in the *Amazon Elastic File System User Guide*.

5. Choose **Edit**. The **File system policy** page appears.
6. In **Policy editor**, enter a policy such as the following, and then choose **Save**.

```
{  
    "Version": "2012-10-17",  
    "Id": "ExamplePolicy01",  
    "Statement": [  
        {  
            "Sid": "ExampleStatement01",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::123456789012:role/rds-efs-integration-role"  
            },  
            "Action": [  
                "elasticfilesystem:ClientMount",  
                "elasticfilesystem:ClientWrite",  
                "elasticfilesystem:ClientRootAccess"  
            ],  
            "Resource": "arn:aws:elasticfilesystem:Region:123456789012:file-  
system/fs-1234567890abcdef0"  
        }  
    ]  
}
```

Step 3: Associate your IAM role with your RDS for Oracle DB instance

In this step, you associate your IAM role with your DB instance. Be aware of the following requirements:

- You must have access to an IAM role with the required Amazon EFS permissions policy attached to it.
- You can associate only one IAM role with your RDS for Oracle DB instance at a time.
- The status of your instance must be **Available**.

For more information, see [Identity and access management for Amazon EFS](#) in the *Amazon Elastic File System User Guide*.

Console

To associate your IAM role with your RDS for Oracle DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Databases**.
3. If your database instance is unavailable, choose **Actions** and then **Start**. When the instance status shows **Started**, go to the next step.
4. Choose the Oracle DB instance name to display its details.

5. On the **Connectivity & security** tab, scroll down to the **Manage IAM roles** section at the bottom of the page.
6. Choose the role to add in the **Add IAM roles to this instance** section.
7. For **Feature**, choose **EFS_INTEGRATION**.
8. Choose **Add role**.

AWS CLI

The following AWS CLI command adds the role to an Oracle DB instance named *mydbinstance*.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-instance \
--db-instance-identifier mydbinstance \
--feature-name EFS_INTEGRATION \
--role-arn your-role-arn
```

For Windows:

```
aws rds add-role-to-db-instance ^
--db-instance-identifier mydbinstance ^
--feature-name EFS_INTEGRATION ^
--role-arn your-role-arn
```

Replace *your-role-arn* with the role ARN that you noted in a previous step. EFS_INTEGRATION must be specified for the --feature-name option.

Adding the EFS_INTEGRATION option

To integrate Amazon RDS for Oracle with Amazon EFS, your DB instance must be associated with an option group that includes the EFS_INTEGRATION option.

Multiple Oracle DB instances that belong to the same option group share the same EFS file system. Different DB instances can access the same data, but access can be divided by using different Oracle directories. For more information see [Transferring files between RDS for Oracle and an Amazon EFS file system \(p. 1681\)](#).

Console

To configure an option group for Amazon EFS integration

1. Create a new option group or identify an existing option group to which you can add the EFS_INTEGRATION option.

For information about creating an option group, see [Creating an option group \(p. 274\)](#).
2. Add the EFS_INTEGRATION option to the option group. You need to specify the EFS_ID file system ID and set the USE_IAM_ROLE flag.

For more information, see [Adding an option to an option group \(p. 277\)](#).
3. Associate the option group with your DB instance in either of the following ways:
 - Create a new Oracle DB instance and associate the option group with it. For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

- Modify an Oracle DB instance to associate the option group with it. For information about modifying an Oracle DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

To configure an option group for EFS integration

1. Create a new option group or identify an existing option group to which you can add the EFS_INTEGRATION option.

For information about creating an option group, see [Creating an option group \(p. 274\)](#).

2. Add the EFS_INTEGRATION option to the option group.

For example, the following AWS CLI command adds the EFS_INTEGRATION option to an option group named **myoptiongroup**.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name myoptiongroup \
--options "OptionName=EFS_INTEGRATION,OptionSettings=\
[{"Name=EFS_ID,Value=fs-1234567890abcdef0},{Name=USE_IAM_ROLE,Value=TRUE}]"
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name myoptiongroup ^
--options "OptionName=EFS_INTEGRATION,OptionSettings=^
[{"Name=EFS_ID,Value=fs-1234567890abcdef0},{Name=USE_IAM_ROLE,Value=TRUE}]"
```

3. Associate the option group with your DB instance in either of the following ways:

- Create a new Oracle DB instance and associate the option group with it. For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- Modify an Oracle DB instance to associate the option group with it. For information about modifying an Oracle DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Configuring Amazon EFS file system permissions

By default, only the root user (UID 0) has read, write, and execute permissions for a newly created EFS file system. For other users to modify the file system, the root user must explicitly grant them access. The user for the RDS for Oracle DB instance is in the `others` category. For more information, see [Working with users, groups, and permissions at the Network File System \(NFS\) Level](#) in the *Amazon Elastic File System User Guide*.

To allow your RDS for Oracle DB instance to read and write files on an EFS file system, do the following:

- Mount an EFS file system locally on your Amazon EC2 instance.
- Configure fine grain permissions.

For example, to grant other users permissions to write to the EFS file system root, run `chmod 777` on this directory. For more information, see [Example Amazon EFS file system use cases and permissions](#) in the *Amazon Elastic File System User Guide*.

Transferring files between RDS for Oracle and an Amazon EFS file system

To transfer files between an RDS for Oracle instance and an Amazon EFS file system, create at least one Oracle directory and configure EFS file system permissions to control DB instance access.

Topics

- [Creating an Oracle directory \(p. 1681\)](#)
- [Transferring data to and from an EFS file system: examples \(p. 1681\)](#)

Creating an Oracle directory

To create an Oracle directory, use the procedure

`rdsadmin.rdsadmin_util.create_directory_efs`. The procedure has the following parameters.

Parameter name	Data type	Default	Required	Description
p_directory_name	VARCHAR2	–	Yes	The name of the Oracle directory.
p_path_on_efs	VARCHAR2	–	Yes	<p>The path on the EFS file system. The prefix of the path name uses the pattern <code>/rdsefs-<i>fsid</i>/</code>, where <i>fsid</i> is a placeholder for your EFS file system ID.</p> <p>For example, if your EFS file system is named <code>fs-1234567890abcdef0</code>, and you create a subdirectory on this file system named <code>mydir</code>, you could specify the following value:</p> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <code>/rdsefs-fs-1234567890abcdef0/mydir</code> </div>

Assume that you create a subdirectory named `/datapump1` on the EFS file system `fs-1234567890abcdef0`. The following example creates an Oracle directory `DATA_PUMP_DIR_EFS` that points to the `/datapump1` directory on the EFS file system. The file system path value for the `p_path_on_efs` parameter is prefixed with the string `/rdsefs-`.

```

BEGIN
    rdsadmin.rdsadmin_util.create_directory_efs(
        p_directory_name => 'DATA_PUMP_DIR_EFS',
        p_path_on_efs     => '/rdsefs-fs-1234567890abcdef0/datapump1');
END;
/

```

Transferring data to and from an EFS file system: examples

The following example uses Oracle Data Pump to export the table named `MY_TABLE` to file `datapump.dmp`. This file resides on an EFS file system.

```

DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'EXPORT', job_mode => 'SCHEMA',
        job_name=>null);
    DBMS_DATAPUMP.ADD_FILE(
        handle      => v_hdnl,

```

```
filename  => 'datapump.dmp',
directory => 'DATA_PUMP_DIR_EFS',
filetype  => dbms_datapump.ku$_file_type_dump_file);
DBMS_DATAPUMP.ADD_FILE(
    handle  => v_hdnl,
    filename  => 'datapump-exp.log',
    directory => 'DATA_PUMP_DIR_EFS',
    filetype  => dbms_datapump.ku$_file_type_log_file);
DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''MY_TABLE''));
DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

The following example uses Oracle Data Pump to import the table named MY_TABLE from file datapump.dmp. This file resides on an EFS file system.

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(
        operation => 'IMPORT',
        job_mode  => 'SCHEMA',
        job_name  => null);
    DBMS_DATAPUMP.ADD_FILE(
        handle  => v_hdnl,
        filename  => 'datapump.dmp',
        directory => 'DATA_PUMP_DIR_EFS',
        filetype  => dbms_datapump.ku$_file_type_dump_file );
    DBMS_DATAPUMP.ADD_FILE(
        handle  => v_hdnl,
        filename  => 'datapump-imp.log',
        directory => 'DATA_PUMP_DIR_EFS',
        filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''MY_TABLE''));
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

For more information, see [Importing data into Oracle on Amazon RDS \(p. 1615\)](#).

Removing the EFS_INTEGRATION option

To remove the EFS_INTEGRATION option from an RDS for Oracle DB instance, do one of the following:

- To remove the EFS_INTEGRATION option from multiple DB instances, remove the EFS_INTEGRATION option from the option group to which the DB instances belong. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove the EFS_INTEGRATION option from a single DB instance, modify the instance and specify a different option group that doesn't include the EFS_INTEGRATION option. You can specify the default (empty) option group or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Troubleshooting Amazon EFS integration

Your RDS for Oracle DB instance monitors the connectivity to an Amazon EFS file system. When monitoring detects an issue, it might try to correct the issue and publish an event in the RDS console. For more information, see [Viewing Amazon RDS events](#).

Use the information in this section to help you diagnose and fix common issues when you work with Amazon EFS integration.

Notification	Description	Action
The EFS for RDS Oracle instance <i>instance_name</i> isn't available on the primary host. NFS port 2049 of your EFS isn't reachable.	The DB instance can't communicate with the EFS file system.	Make sure of the following: <ul style="list-style-type: none"> The EFS file system exists. The security group that is attached to the EFS mount target has an inbound rule to allow the security group or network subnet of the RDS for Oracle DB instance on TCP/2049 (Type NFS).
The EFS isn't reachable.	An error occurred during the installation of the EFS_INTEGRATION option.	Make sure of the following: <ul style="list-style-type: none"> The EFS file system exists. The security group that is attached to the EFS mount target has an inbound rule to allow the security group or network subnet of the RDS for Oracle DB instance on TCP/2049 (Type NFS). The enableDnsSupport attribute is turned on for your VPC.
The associated role with your DB instance wasn't found.	An error occurred during the installation of the EFS_INTEGRATION option.	Make sure that you associated an IAM role with your RDS for Oracle DB instance.
N/A	You might see the following error: PLSQL-00302: component 'CREATE_DIRECTORY_EFS' must be declared. This error can occur when you're using a version of RDS for Oracle that doesn't support Amazon EFS.	Make sure that you are using RDS for Oracle DB instance version 19.0.0.0.ru-2022-07.rur-2022-07.r1 or higher.
Read access of your EFS is denied. Check your file system policy.	Your DB instance can't read the EFS file system.	Make sure that your EFS file system allows read access through the IAM role or on the EFS file system level.
N/A	Your DB instance can't write to the EFS file system.	Take the following steps: <ol style="list-style-type: none"> 1. Make sure that your EFS file system is mounted on an Amazon EC2 instance. 2. Give the others group write access to your RDS user. The simplest technique is to run the chmod 777 command on

Notification	Description	Action
		the top directory of the EFS file system.

Oracle Java virtual machine

Amazon RDS supports Oracle Java Virtual Machine (JVM) through the use of the JVM option. Oracle Java provides a SQL schema and functions that facilitate Oracle Java features in an Oracle database. For more information, see [Introduction to Java in Oracle database](#) in the Oracle documentation.

You can use Oracle JVM with the following Oracle Database versions:

- Oracle Database 21c (21.0.0), all versions
- Oracle Database 19c (19.0.0), all versions
- Oracle Database 12c Release 2 (12.2), all versions
- Oracle Database 12c Release 1 (12.1), version 12.1.0.2.v13 and higher

Java implementation in Amazon RDS has a limited set of permissions. The master user is granted the RDS_JAVA_ADMIN role, which grants a subset of the privileges granted by the JAVA_ADMIN role. To list the privileges granted to the RDS_JAVA_ADMIN role, run the following query on your DB instance:

```
SELECT * FROM dba_java_policy
WHERE grantee IN ('RDS_JAVA_ADMIN', 'PUBLIC')
AND enabled = 'ENABLED'
ORDER BY type_name, name, grantee;
```

Prerequisites for Oracle JVM

The following are prerequisites for using Oracle Java:

- Your DB instance must be of a large enough class. Oracle Java isn't supported for the db.t3.micro or db.t3.small DB instance classes. For more information, see [DB instance classes \(p. 10\)](#).
- Your DB instance must have **Auto Minor Version Upgrade** enabled. This option enables your DB instance to receive minor DB engine version upgrades automatically when they become available. Amazon RDS uses this option to update your DB instance to the latest Oracle Patch Set Update (PSU) or Release Update (RU). For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Best practices for Oracle JVM

The following are best practices for using Oracle Java:

- For maximum security, use the JVM option with Secure Sockets Layer (SSL). For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).
- Configure your DB instance to restrict network access. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#) and [Working with a DB instance in a VPC \(p. 2103\)](#).
- Update the configuration of your HTTPS endpoints to support TLSv1.2 if you meet the following conditions:
 - You use Oracle Java Virtual Machine (JVM) to connect an HTTPS endpoint over TLSv1 or TLSv1.1 protocols.
 - Your endpoint doesn't support the TLSv1.2 protocol.
 - You haven't applied the April 2021 release update to your Oracle DB.

By updating your endpoint configuration, you ensure that the connectivity of the JVM to the HTTPS endpoint will continue to work. For more information about TLS changes in the Oracle JRE and JDK, see [Oracle JRE and JDK Cryptographic Roadmap](#).

Adding the Oracle JVM option

The following is the general process for adding the JVM option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

There is a brief outage while the JVM option is added. After you add the option, you don't need to restart your DB instance. As soon as the option group is active, Oracle Java is available.

Note

During this outage, password verification functions are disabled briefly. You can also expect to see events related to password verification functions during the outage. Password verification functions are enabled again before the Oracle DB instance is available.

To add the JVM option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - For **Engine**, choose the DB engine used by the DB instance (**oracle-ee**, **oracle-se**, **oracle-se1**, or **oracle-se2**).
 - For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **JVM** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
4. Grant the required permissions to users.

The Amazon RDS master user has the permissions to use the JVM option by default. If other users require these permissions, connect to the DB instance as the master user in a SQL client and grant the permissions to the users.

The following example grants the permissions to use the JVM option to the `test_proc` user.

```
create user test_proc identified by password;
CALL dbms_java.grant_permission('TEST_PROC',
  'oracle.aurora.security.JServerPermission', 'LoadClassInPackage.*', '');
```

After the user is granted the permissions, the following query should return output.

```
select * from dba_java_policy where grantee='TEST_PROC';
```

Note

The Oracle user name is case-sensitive, and it usually has all uppercase characters.

Removing the Oracle JVM option

You can remove the JVM option from a DB instance. There is a brief outage while the option is removed. After you remove the JVM option, you don't need to restart your DB instance.

Warning

Removing the JVM option can result in data loss if the DB instance is using data types that were enabled as part of the option. Back up your data before proceeding. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

To remove the JVM option from a DB instance, do one of the following:

- Remove the JVM option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- Modify the DB instance and specify a different option group that doesn't include the JVM option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Enterprise Manager

Amazon RDS supports Oracle Enterprise Manager (OEM). OEM is the Oracle product line for integrated management of enterprise information technology.

Amazon RDS supports OEM through the following options.

Option	Option ID	Supported OEM releases	Supported Oracle Database releases
OEM Database Express (p. 1689)	OEM	OEM Database Express 12c	Oracle Database 19c (non-CDB only) and Oracle Database 12c
OEM Management Agent (p. 1693)	OEM_AGENT	OEM Cloud Control for 13c OEM Cloud Control for 12c	Oracle Database 19c (non-CDB only) and Oracle Database 12c

Note

You can use OEM Database or OEM Management Agent, but not both.

Note

These options aren't supported for the single-tenant architecture.

Oracle Enterprise Manager Database Express

Amazon RDS supports Oracle Enterprise Manager (OEM) Database Express through the use of the OEM option. Amazon RDS supports Oracle Enterprise Manager Database Express for the following releases:

- Oracle Database 19c (non-CDB only)
- Oracle Database 12c

OEM Database Express and Database Control are similar tools that have a web-based interface for Oracle database administration. For more information about these tools, see [Accessing Enterprise Manager database Express 18c](#) and [Accessing Enterprise Manager Database Express 12c](#) in the Oracle documentation.

The following is a limitation for OEM Database Express:

- OEM Database Express isn't supported on the db.t3.micro or db.t3.small DB instance classes.

For more information about DB instance classes, see [RDS for Oracle instance classes \(p. 1477\)](#).

OEM Database option settings

Amazon RDS supports the following settings for the OEM option.

Option setting	Valid values	Description
Port	An integer value	The port on the DB instance that listens for OEM Database. The default for OEM Database Express is 5500.
Security Groups	—	A security group that has access to Port .

Adding the OEM Database option

The general process for adding the OEM option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

When you add the OEM option for an Oracle Database 12c or later DB instance, a brief outage occurs while your DB instance is automatically restarted.

To add the OEM option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine** choose the oracle edition for your DB instance.
 - b. For **Major engine version** choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the OEM option to the option group, and configure the option settings. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#). For more information about each setting, see [OEM Database option settings \(p. 1689\)](#).

Note

If you add the OEM option to an existing option group that is already attached to one or more Oracle Database 19c (non-CDB only) or Oracle Database 12c DB instances, a brief outage occurs while all the DB instances are automatically restarted.

3. Apply the option group to a new or existing DB instance:

- For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. When you add the OEM option for an Oracle Database 19c (non-CDB only) or Oracle Database 12c DB instance, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Note

You can also use the AWS CLI to add the OEM option. For examples, see [Adding an option to an option group \(p. 277\)](#).

Accessing OEM through your browser

After you enable the OEM option, you can begin using the OEM Database tool from your web browser.

You can access either OEM Database Control or OEM Database Express from your web browser. For example, if the endpoint for your Amazon RDS DB instance is `mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com`, and your OEM port is 1158, then the URL to access the OEM Database Control the following.

```
https://mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com:1158/em
```

When you access either tool from your web browser, a login window appears that prompts you for a user name and password. Type the master user name and master password for your DB instance. You are now ready to manage your Oracle databases.

Modifying OEM Database settings

After you enable OEM Database, you can modify the Security Groups setting for the option.

You can't modify the OEM port number after you have associated the option group with a DB instance. To change the OEM port number for a DB instance, do the following:

1. Create a new option group.
2. Add the OEM option with the new port number to the new option group.
3. Remove the existing option group from the DB instance.
4. Add the new option group to the DB instance.

For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [OEM Database option settings \(p. 1689\)](#).

Running OEM Database Express tasks

You can use Amazon RDS procedures to run certain OEM Database Express tasks. By running these procedures, you can do the tasks listed following.

Note

OEM Database Express tasks run asynchronously.

Tasks

- [Switching the website front end for OEM Database Express to Adobe Flash \(p. 1691\)](#)
- [Switching the website front end for OEM Database Express to Oracle JET \(p. 1692\)](#)

Switching the website front end for OEM Database Express to Adobe Flash

Note

This task is available only for Oracle Database 19c non-CDBs.

Starting with Oracle Database 19c, Oracle has deprecated the former OEM Database Express user interface, which was based on Adobe Flash. Instead, OEM Database Express now uses an interface built with Oracle JET. If you experience difficulties with the new interface, you can switch back to the deprecated Flash-based interface. Difficulties you might experience with the new interface include being stuck on a Loading screen after logging in to OEM Database Express. You might also miss certain features that were present in the Flash-based version of OEM Database Express.

To switch the OEM Database Express website front end to Adobe Flash, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash`. This procedure is equivalent to the `execemx emx` SQL command.

Security best practices discourage the use of Adobe Flash. Although you can revert to the Flash-based OEM Database Express, we recommend the use of the JET-based OEM Database Express websites if possible. If you revert to using Adobe Flash and want to switch back to using Oracle JET, use the `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet` procedure. After an Oracle database upgrade, a newer version of Oracle JET might resolve JET-related issues in OEM Database Express. For more information about switching to Oracle JET, see [Switching the website front end for OEM Database Express to Oracle JET \(p. 1692\)](#).

Note

Running this task from the source DB instance for a read replica also causes the read replica to switch its OEM Database Express website front ends to Adobe Flash.

The following procedure invocation creates a task to switch the OEM Database Express website to Adobe Flash and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash() as TASK_ID from DUAL;
```

You can view the result by displaying the task's output file.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP', 'dbtask-task-id.log'));
```

Replace `task-id` with the task ID returned by the procedure. For more information about the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`, see [Reading files in a DB instance directory \(p. 1598\)](#).

You can also view the contents of the task's output file in the AWS Management Console by searching the log entries in the **Logs & events** section for the task-id.

Switching the website front end for OEM Database Express to Oracle JET

Note

This task is available only for Oracle Database 19c non-CDBs.

To switch the OEM Database Express website front end to Oracle JET, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. This procedure is equivalent to the `execemx_omx` SQL command.

By default, the OEM Database Express websites for Oracle DB instances running 19c or later use Oracle JET. If you used the `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash` procedure to switch the OEM Database Express website front end to Adobe Flash, you can switch back to Oracle JET. To do this, use the `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet` procedure. For more information about switching to Adobe Flash, see [Switching the website front end for OEM Database Express to Adobe Flash \(p. 1691\)](#).

Note

Running this task from the source DB instance for a read replica also causes the read replica to switch its OEM Database Express website front ends to Oracle JET.

The following procedure invocation creates a task to switch the OEM Database Express website to Oracle JET and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet() as TASK_ID from DUAL;
```

You can view the result by displaying the task's output file.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-id.log'));
```

Replace `task-id` with the task ID returned by the procedure. For more information about the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`, see [Reading files in a DB instance directory \(p. 1598\)](#).

You can also view the contents of the task's output file in the AWS Management Console by searching the log entries in the **Logs & events** section for the task-id.

Removing the OEM Database option

You can remove the OEM option from a DB instance. When you remove the OEM option for an Oracle Database 12c or later DB instance, a brief outage occurs while your instance is automatically restarted. Therefore, after you remove the OEM option, you don't need to restart your DB instance.

To remove the OEM option from a DB instance, do one of the following:

- Remove the OEM option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- Modify the DB instance and specify a different option group that doesn't include the OEM option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Management Agent for Enterprise Manager Cloud Control

Oracle Enterprise Manager (OEM) Management Agent is a software component that monitors targets running on hosts and communicates that information to the middle-tier Oracle Management Service (OMS). For more information, see [Overview of Oracle Enterprise Manager cloud control 12c](#) and [Overview of Oracle Enterprise Manager cloud control 13c](#) in the Oracle documentation.

Amazon RDS supports Management Agent through the use of the OEM_AGENT option. Management Agent requires an Amazon RDS DB instance running any of the following releases:

- Oracle Database 19c (19.0.0.0) using the non-CDB architecture
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Amazon RDS supports Management Agent for the following versions of OEM:

- Oracle Enterprise Manager Cloud Control for 13c
- Oracle Enterprise Manager Cloud Control for 12c

Topics

- [Prerequisites for Management Agent \(p. 1693\)](#)
- [Limitations for Management Agent \(p. 1695\)](#)
- [Option settings for Management Agent \(p. 1695\)](#)
- [Adding the Management Agent option \(p. 1697\)](#)
- [Using the Management Agent \(p. 1698\)](#)
- [Modifying Management Agent settings \(p. 1699\)](#)
- [Performing database tasks with the Management Agent \(p. 1699\)](#)
- [Removing the Management Agent option \(p. 1702\)](#)

Prerequisites for Management Agent

To use Management Agent, ensure that you meet the following prerequisites.

General prerequisites

Following are general prerequisites for using Management Agent:

- You need an Oracle Management Service (OMS) that is configured to connect to your Amazon RDS DB instance.
- In most cases, you must configure your VPC to allow connections from OMS to your DB instance. If you aren't familiar with Amazon Virtual Private Cloud (Amazon VPC), we recommend that you complete the steps in [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#) before continuing.
- Management Agent version 13.5.0.0.v1 requires OMS version 13.5.0.0 or later.
- Management Agent version 13.4.0.9.v1 requires OMS version 13.4.0.9 or later and patch 32198287.
- Ensure that you have sufficient storage space for your OEM release:
 - At least 8.5 GiB for OEM 13c Release 5
 - At least 8.5 GiB for OEM 13c Release 4
 - At least 8.5 GiB for OEM 13c Release 3
 - At least 5.5 GiB for OEM 13c Release 2

- At least 4.5 GiB OEM 13c Release 1
- At least 2.5 GiB for OEM 12c
- If you are using Management Agent versions OEM_AGENT 13.2.0.0.v3 and 13.3.0.0.v2, and if you want to use TCPS connectivity, follow the instructions in [Configuring third party CA certificates for communication with target databases](#) in the Oracle documentation. Also, update the JDK on your OMS by following the instructions in the Oracle document with the Oracle Doc ID 2241358.1. This step ensures that OMS supports all the cipher suites that the database supports.

Note

TCPS connectivity between the Management Agent and the DB instance is only supported for Management Agent versions OEM_AGENT 13.2.0.0.v3 and 13.3.0.0.v2.

Oracle Database release prerequisites

Following are the supported Oracle Database versions for each Management Agent version.

Management Agent version	Oracle Database 19c using the non-CDB architecture	Oracle Database 12c Release 2 (12.2)	Oracle Database 12c Release 1 (12.1)
13.5.0.0.v1	Supported	Supported	Supported
13.4.0.9.v1	Supported	Supported	Supported
13.3.0.0.v2	Supported	Supported	Supported
13.3.0.0.v1	Supported	Supported	Supported
13.2.0.0.v3	Supported	Supported	Supported
13.2.0.0.v2	Supported	Supported	Supported
13.2.0.0.v1	Supported	Supported	Supported
13.1.0.0.v1	Supported	Supported	Supported
12.1.0.5.v1	Not supported	Supported	Supported
12.1.0.4.v1	Not supported	Supported	Supported

Following are prerequisites for different database versions:

- For an Amazon RDS DB instance running Oracle Database 19c (19.0.0.0), the minimum AGENT_VERSION is 13.1.0.0.v1.
- For an Amazon RDS DB instance running Oracle Database Release 2 (12.2.0.1) or lower, meet the following requirements:

- For OMS 13c Release 2 with Oracle patch 25163555 applied, use OEM Agent 13.2.0.0.v2 or later.

Use OMSPatcher to apply the patch.

- For unpatched OMS 13c Release 2, use OEM Agent 13.2.0.0.v1.

Use OMSPatcher to apply patches.

OMS host communication prerequisites

Make sure that your OMS host and your Amazon RDS DB instance can communicate. Do the following:

- To connect from the Management Agent to your OMS, if your OMS is behind a firewall, add the IP addresses of your DB instances to your OMS.

Make sure the firewall for the OMS allows traffic from both the DB listener port (default 1521) and the OEM Agent port (default 3872), originating from the IP address of the DB instance.

- To connect from your OMS to the Management Agent, if your OMS has a publicly resolvable host name, add the OMS address to a security group. Your security group must have inbound rules that allow access to the DB listener port and the Management Agent port. For an example of creating a security and adding inbound rules, see [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).
- To connect from your OMS to the Management Agent, if your OMS doesn't have a publicly resolvable host name, use one of the following:
 - If your OMS is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance in a private VPC, you can set up VPC peering to connect from OMS to Management Agent. For more information, see [A DB instance in a VPC accessed by an EC2 instance in a different VPC \(p. 2117\)](#).
 - If your OMS is hosted on-premises, you can set up a VPN connection to allow access from OMS to Management Agent. For more information, see [A DB instance in a VPC accessed by a client application through the internet \(p. 2118\)](#) or [VPN connections](#).

Limitations for Management Agent

Following are some limitations to using Management Agent:

- Administrative tasks such as job execution and database patching, that require host credentials, aren't supported.
- Host metrics and the process list aren't guaranteed to reflect the actual system state. Thus, you shouldn't use OEM to monitor the root file system or mount point file system. For more information about monitoring the operating system, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).
- Autodiscovery isn't supported. You must manually add database targets.
- OMS module availability depends on your database edition. For example, the database performance diagnosis and tuning module is only available for Oracle Database Enterprise Edition.
- Management Agent consumes additional memory and computing resources. If you experience performance problems after enabling the OEM_AGENT option, we recommend that you scale up to a larger DB instance class. For more information, see [DB instance classes \(p. 10\)](#) and [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- The user running the OEM_AGENT on the Amazon RDS host doesn't have operating system access to the alert log. Thus, you can't collect metrics for DB Alert Log and DB Alert Log Error Status in OEM.

Option settings for Management Agent

Amazon RDS supports the following settings for the Management Agent option.

Option setting	Required	Valid values	Description
Version (AGENT_VERSION)	Yes	13.5.0.0.v1 13.4.0.9.v1 13.3.0.0.v2 13.3.0.0.v1 13.2.0.0.v3	The version of the Management Agent software. The AWS CLI option name is OptionVersion. Note In the AWS GovCloud (US) Regions, 12.1 and 13.1 versions aren't available.

Option setting	Required	Valid values	Description
		13.2.0.0.v2 13.2.0.0.v1 13.1.0.0.v1 12.1.0.5.v1 12.1.0.4.v1	
Port (AGENT_PORT)	Yes	An integer value	The port on the DB instance that listens for the OMS host. The default is 3872. Your OMS host must belong to a security group that has access to this port. The AWS CLI option name is Port.
Security Groups	Yes	Existing security groups	A security group that has access to Port . Your OMS host must belong to this security group. The AWS CLI option name is VpcSecurityGroupMemberships or DBSecurityGroupMemberships.
OMS_HOST	Yes	A string value, for example <i>my.example.oms</i>	The publicly accessible host name or IP address of the OMS. The AWS CLI option name is OMS_HOST.
OMS_PORT	Yes	An integer value	The HTTPS upload port on the OMS Host that listens for the Management Agent. To determine the HTTPS upload port, connect to the OMS host, and run the following command (which requires the SYSMAN password): <code>emctl status oms -details</code> The AWS CLI option name is OMS_PORT.
AGENT_REGISTRATION_PASSWORD	string value		The password that the Management Agent uses to authenticate itself with the OMS. We recommend that you create a persistent password in your OMS before enabling the OEM_AGENT option. With a persistent password you can share a single Management Agent option group among multiple Amazon RDS databases. The AWS CLI option name is AGENT_REGISTRATION_PASSWORD.
ALLOW_TLS_ONLY	No	true, false (default)	A value that configures the OEM Agent to support only the TLSv1 protocol while the agent listens as a server. This setting is only supported for 12.1 agent versions. Later agent versions only support Transport Layer Security (TLS) by default.

Option setting	Required	Valid values	Description
MINIMUM_TLS_VERSION		TLSv1 (default), TLSv1.2	A value that specifies the minimum TLS version supported by the OEM Agent while the agent listens as a server. This setting is only supported for agent versions 13.1.0.0.v1 and higher. Earlier agent versions only support the TLSv1 setting.
TLS_CIPHER_SUITE		TLS_RSA_WITH_AES_128_CBC_SHA (Default supported by all agent versions)	Specifies the TLS cipher suite used by the OEM Agent while the agent listens as a server.
		TLS_RSA_WITH_AES_128_CBC_SHA256 (Requires version 13.1.0.0.v1 or above)	
		TLS_RSA_WITH_AES_256_CBC_SHA (Requires version 13.2.0.0.v3 or above)	
		TLS_RSA_WITH_AES_256_CBC_SHA256 (Requires version 13.2.0.0.v3 or above)	

Adding the Management Agent option

The general process for adding the Management Agent option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

If you encounter errors, check [My Oracle Support](#) documents for information about resolving specific problems.

After you add the Management Agent option, you don't need to restart your DB instance. As soon as the option group is active, the OEM Agent is active.

If your OMS host is using an untrusted third-party certificate, Amazon RDS returns the following error.

You successfully installed the OEM_AGENT option. Your OMS host is using an untrusted third party certificate.
Configure your OMS host with the trusted certificates from your third party.

If this error is returned, the Management Agent option isn't enabled until the problem is corrected. For information about correcting the problem, see the My Oracle Support document [2202569.1](#).

Console

To add the Management Agent option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine** choose the oracle edition for your DB instance.
 - b. For **Major engine version** choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **OEM_AGENT** option to the option group, and configure the option settings. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#). For more information about each setting, see [Option settings for Management Agent \(p. 1695\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

The following example uses the AWS CLI `add-option-to-option-group` command to add the OEM_AGENT option to an option group called `myoptiongroup`.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name "myoptiongroup" \
--options \
  OptionName=OEM_AGENT,OptionVersion=13.1.0.0.v1,Port=3872,VpcSecurityGroupMemberships=sg-1234567890,Opt \
  {Name=OMS_PORT,Value=4903},{Name=AGENT_REGISTRATION_PASSWORD,Value=password}] \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name "myoptiongroup" ^
--options \
  OptionName=OEM_AGENT,OptionVersion=13.1.0.0.v1,Port=3872,VpcSecurityGroupMemberships=sg-1234567890,Opt \
  {Name=OMS_PORT,Value=4903},{Name=AGENT_REGISTRATION_PASSWORD,Value=password}] ^
--apply-immediately
```

Using the Management Agent

After you enable the Management Agent option, take the following steps to begin using it.

To use the Management Agent

1. Unlock and reset the DBSNMP account credential. Do this by running the following code on your target database on your DB instance and using your master user account.

```
ALTER USER dbsnmp IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

2. Add your targets to the OMS console manually:
 - a. In your OMS console, choose **Setup, Add Target, Add Targets Manually**.
 - b. Choose **Add Targets Declaratively by Specifying Target Monitoring Properties**.
 - c. For **Target Type**, choose **Database Instance**.
 - d. For **Monitoring Agent**, choose the agent with the identifier that is the same as your RDS DB instance identifier.
 - e. Choose **Add Manually**.
 - f. Enter the endpoint for the Amazon RDS DB instance, or choose it from the host name list. Make sure that the specified host name matches the endpoint of the Amazon RDS DB instance.

For information about finding the endpoint for your Amazon RDS DB instance, see [Finding the endpoint of your Oracle DB instance \(p. 1488\)](#).
 - g. Specify the following database properties:
 - For **Target name**, enter a name.
 - For **Database system name**, enter a name.
 - For **Monitor username**, enter **dbsnmp**.
 - For **Monitor password**, enter the password from step 1.
 - For **Role**, enter **normal**.
 - For **Oracle home path**, enter **/oracle**.
 - For **Listener Machine name**, the agent identifier already appears.
 - For **Port**, enter the database port. The RDS default port is 1521.
 - For **Database name**, enter the name of your database.
 - h. Choose **Test Connection**.
 - i. Choose **Next**. The target database appears in your list of monitored resources.

Modifying Management Agent settings

After you enable the Management Agent, you can modify settings for the option. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [Option settings for Management Agent \(p. 1695\)](#).

Performing database tasks with the Management Agent

You can use Amazon RDS procedures to run certain EMCTL commands on the Management Agent. By running these procedures, you can do the tasks listed following.

Note

Tasks are executed asynchronously.

Tasks

- [Getting the status of the Management Agent \(p. 1700\)](#)
- [Restarting the Management Agent \(p. 1700\)](#)
- [Listing the targets monitored by the Management Agent \(p. 1700\)](#)
- [Listing the collection threads monitored by the Management Agent \(p. 1700\)](#)
- [Clearing the Management Agent state \(p. 1701\)](#)
- [Making the Management Agent upload its OMS \(p. 1701\)](#)
- [Pinging the OMS \(p. 1701\)](#)
- [Viewing the status of an ongoing task \(p. 1701\)](#)

Getting the status of the Management Agent

To get the status of the Management Agent, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent`. This procedure is equivalent to the `emctl status agent` command.

The following procedure creates a task to get the Management Agent's status and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent() as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Restarting the Management Agent

To restart the Management Agent, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.restart_oem_agent`. This procedure is equivalent to running the `emctl stop agent` and `emctl start agent` commands.

The following procedure creates a task to restart the Management Agent and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.restart_oem_agent as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Listing the targets monitored by the Management Agent

To list the targets monitored by the Management Agent, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent`. This procedure is equivalent to running the `emctl config agent listtargets` command.

The following procedure creates a task to list the targets monitored by the Management Agent and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Listing the collection threads monitored by the Management Agent

To list of all the running, ready, and scheduled collection threads monitored by the Management Agent, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent`. This procedure is equivalent to the `emctl status agent scheduler` command.

The following procedure creates a task to list the collection threads and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent() as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Clearing the Management Agent state

To clear the Management Agent's state, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent`. This procedure is equivalent to running the `emctl clearstate agent` command.

The following procedure creates a task that clears the Management Agent's state and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent() as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Making the Management Agent upload its OMS

To make the Management Agent upload the Oracle Management Server (OMS) associated with it, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent`. This procedure is equivalent to running the `emctl upload agent` command.

The following procedure creates a task that makes the Management Agent upload its associated OMS and return the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent() as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Pinging the OMS

To ping the Management Agent's OMS, run the Amazon RDS procedure `rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent`. This procedure is equivalent to running the `emctl pingOMS` command.

The following procedure creates a task that pings the Management Agent's OMS and returns the ID of the task.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent() as TASK_ID from DUAL;
```

To view the result by displaying the task's output file, see [Viewing the status of an ongoing task \(p. 1701\)](#).

Viewing the status of an ongoing task

You can view the status of an ongoing task in a bdump file. The bdump files are located in the `/rdsdbdata/log/trace` directory. Each bdump file name is in the following format.

```
dbtask-task-id.log
```

When you want to monitor a task, replace `task-id` with the ID of the task that you want to monitor.

To view the contents of bdump files, run the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`. The following query returns the contents of the `dbtask-1546988886389-2444.log` bdump file.

```
SELECT text FROM
table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1546988886389-2444.log'));
```

For more information about the Amazon RDS procedure `rdsadmin.rds_file_util.read_text_file`, see [Reading files in a DB instance directory \(p. 1598\)](#).

Removing the Management Agent option

You can remove the OEM Agent from a DB instance. After you remove the OEM Agent, you don't need to restart your DB instance.

To remove the OEM Agent from a DB instance, do one of the following:

- Remove the OEM Agent option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- Modify the DB instance and specify a different option group that doesn't include the OEM Agent option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Label Security

Amazon RDS supports Oracle Label Security for the Enterprise Edition of Oracle Database through the use of the OLS option.

Most database security controls access at the object level. Oracle Label Security provides fine-grained control of access to individual table rows. For example, you can use Label Security to enforce regulatory compliance with a policy-based administration model. You can use Label Security policies to control access to sensitive data, and restrict access to only users with the appropriate clearance level. For more information, see [Introduction to Oracle Label Security](#) in the Oracle documentation.

Topics

- [Prerequisites for Oracle Label Security \(p. 1703\)](#)
- [Adding the Oracle Label Security option \(p. 1703\)](#)
- [Using Oracle Label Security \(p. 1704\)](#)
- [Removing the Oracle Label Security option \(p. 1704\)](#)
- [Troubleshooting \(p. 1705\)](#)

Prerequisites for Oracle Label Security

Familiarize yourself with the following prerequisites for Oracle Label Security:

- Your DB instance must use the Bring Your Own License model. For more information, see [RDS for Oracle licensing options \(p. 1474\)](#).
- You must have a valid license for Oracle Enterprise Edition with Software Update License and Support.
- Your Oracle license must include the Label Security option.
- You must be using the non-multitenant database architecture rather than the single-tenant architecture. For more information, see [RDS for Oracle architecture \(p. 1480\)](#).

Adding the Oracle Label Security option

The general process for adding the Oracle Label Security option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.

Important

Oracle Label Security is a permanent and persistent option.

3. Associate the option group with the DB instance.

After you add the Label Security option, as soon as the option group is active, Label Security is active.

To add the label security option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose **oracle-ee**.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **OLS** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).

Important

If you add Label Security to an existing option group that is already attached to one or more DB instances, all the DB instances are restarted.

3. Apply the option group to a new or existing DB instance:

- For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. When you add the Label Security option to an existing DB instance, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Using Oracle Label Security

To use Oracle Label Security, you create policies that control access to specific rows in your tables. For more information, see [Creating an Oracle Label Security policy](#) in the Oracle documentation.

When you work with Label Security, you perform all actions as the LBAC_DBA role. The master user for your DB instance is granted the LBAC_DBA role. You can grant the LBAC_DBA role to other users so that they can administer Label Security policies.

For the following releases, make sure to grant access to the OLS_ENFORCEMENT package to any new users who require access to Oracle Label Security:

- Oracle Database 19c using the non-CDB architecture
- Oracle Database 12c Release 2 (12.2)

To grant access to the OLS_ENFORCEMENT package, connect to the DB instance as the master user and run the following SQL statement:

```
GRANT ALL ON LBACSYS.OLS_ENFORCEMENT TO username;
```

You can configure Label Security through the Oracle Enterprise Manager (OEM) Cloud Control. Amazon RDS supports the OEM Cloud Control through the Management Agent option. For more information, see [Oracle Management Agent for Enterprise Manager Cloud Control \(p. 1693\)](#).

Removing the Oracle Label Security option

You can remove Oracle Label Security from a DB instance.

To remove Label Security from a DB instance, do one of the following:

- To remove Label Security from multiple DB instances, remove the Label Security option from the option group they belong to. This change affects all DB instances that use the option group. When you remove Label Security from an option group that is attached to multiple DB instances, all the DB instances are restarted. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove Label Security from a single DB instance, modify the DB instance and specify a different option group that doesn't include the Label Security option. You can specify the default (empty) option group, or a different custom option group. When you remove the Label Security option, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Troubleshooting

The following are issues you might encounter when you use Oracle Label Security.

Issue	Troubleshooting suggestions
When you try to create a policy, you see an error message similar to the following: insufficient authorization for the SYSDBA package.	A known issue with Oracle's Label Security feature prevents users with usernames of 16 or 24 characters from running Label Security commands. You can create a new user with a different number of characters, grant LBAC_DBA to the new user, log in as the new user, and run the OLS commands as the new user. For additional information, please contact Oracle support.

Oracle Locator

Amazon RDS supports Oracle Locator through the use of the LOCATOR option. Oracle Locator provides capabilities that are typically required to support internet and wireless service-based applications and partner-based GIS solutions. Oracle Locator is a limited subset of Oracle Spatial. For more information, see [Oracle Locator](#) in the Oracle documentation.

Important

If you use Oracle Locator, Amazon RDS automatically updates your DB instance to the latest Oracle PSU if there are security vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9+ or other announced security vulnerabilities.

Amazon RDS supports Oracle Locator for the following releases of Oracle Database:

- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1), version 12.1.0.2.v13 or later

Oracle Locator isn't supported for Oracle Database 21c, but its functionality is available in the Oracle Spatial option. Formerly, the Spatial option required additional licenses. Oracle Locator represented a subset of Oracle Spatial features and didn't require additional licenses. In 2019, Oracle announced that all Oracle Spatial features were included in the Enterprise Edition and Standard Edition Two licenses without additional cost. Consequently, the Oracle Spatial option no longer required additional licensing.

Starting with Oracle Database 21c, the Oracle Locator option is no longer supported. To use the Oracle Locator features in Oracle Database 21c, install the Oracle Spatial option instead. For more information, see [Machine Learning, Spatial and Graph - No License Required!](#) in the Oracle Database Insider blog.

Prerequisites for Oracle Locator

The following are prerequisites for using Oracle Locator:

- Your DB instance must be of sufficient class. Oracle Locator is not supported for the db.t3.micro or db.t3.small DB instance classes. For more information, see [RDS for Oracle instance classes \(p. 1477\)](#).
- Your DB instance must have **Auto Minor Version Upgrade** enabled. This option enables your DB instance to receive minor DB engine version upgrades automatically when they become available and is required for any options that install the Oracle Java Virtual Machine (JVM). Amazon RDS uses this option to update your DB instance to the latest Oracle Patch Set Update (PSU) or Release Update (RU). For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Best practices for Oracle Locator

The following are best practices for using Oracle Locator:

- For maximum security, use the LOCATOR option with Secure Sockets Layer (SSL). For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).
- Configure your DB instance to restrict access to your DB instance. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#) and [Working with a DB instance in a VPC \(p. 2103\)](#).

Adding the Oracle Locator option

The following is the general process for adding the LOCATOR option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.

2. Add the option to the option group.
3. Associate the option group with the DB instance.

If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the LOCATOR option is added. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you add the option, you don't need to restart your DB instance. As soon as the option group is active, Oracle Locator is available.

Note

During this outage, password verification functions are disabled briefly. You can also expect to see events related to password verification functions during the outage. Password verification functions are enabled again before the Oracle DB instance is available.

To add the LOCATOR option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose the oracle edition for your DB instance.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the LOCATOR option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Using Oracle Locator

After you enable the Oracle Locator option, you can begin using it. You should only use Oracle Locator features. Don't use any Oracle Spatial features unless you have a license for Oracle Spatial.

For a list of features that are supported for Oracle Locator, see [Features Included with Locator](#) in the Oracle documentation.

For a list of features that are not supported for Oracle Locator, see [Features Not Included with Locator](#) in the Oracle documentation.

Removing the Oracle Locator option

After you drop all objects that use data types provided by the LOCATOR option, you can remove the option from a DB instance. If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the LOCATOR option is removed. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you remove the LOCATOR option, you don't need to restart your DB instance.

To drop the LOCATOR option

1. Back up your data.

Warning

If the instance uses data types that were enabled as part of the option, and if you remove the LOCATOR option, you can lose data. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

2. Check whether any existing objects reference data types or features of the LOCATOR option.

If LOCATOR options exist, the instance can get stuck when applying the new option group that doesn't have the LOCATOR option. You can identify the objects by using the following queries:

```
SELECT OWNER, SEGMENT_NAME, TABLESPACE_NAME, BYTES/1024/1024 mbytes
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE '%TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
       (SELECT DISTINCT OWNER, TABLE_NAME
        FROM   DBA_TAB_COLUMNS
        WHERE  DATA_TYPE='SDO_Geometry'
        AND    OWNER <> 'MDSYS')
ORDER BY 1,2,3,4;

SELECT OWNER, TABLE_NAME, COLUMN_NAME
FROM   DBA_TAB_COLUMNS
WHERE  DATA_TYPE = 'SDO_Geometry'
AND    OWNER <> 'MDSYS'
ORDER BY 1,2,3;
```

3. Drop any objects that reference data types or features of the LOCATOR option.
4. Do one of the following:
 - Remove the LOCATOR option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
 - Modify the DB instance and specify a different option group that doesn't include the LOCATOR option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Multimedia

Amazon RDS supports Oracle Multimedia through the use of the MULTIMEDIA option. You can use Oracle Multimedia to store, manage, and retrieve images, audio, video, and other heterogeneous media data. For more information, see [Oracle Multimedia](#) in the Oracle documentation.

Important

If you use Oracle Multimedia, Amazon RDS automatically updates your DB instance to the latest Oracle PSU if there are security vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9+ or other announced security vulnerabilities.

Amazon RDS supports Oracle Multimedia for all editions of the following versions:

- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1), version 12.1.0.2.v13 or higher

Note

Oracle desupported Oracle Multimedia in Oracle Database 19c. So, Oracle Multimedia isn't supported for Oracle Database 19c DB instances. For more information, see [Desupport of Oracle Multimedia](#) in the Oracle documentation.

Prerequisites for Oracle Multimedia

The following are prerequisites for using Oracle Multimedia:

- Your DB instance must be of sufficient class. Oracle Multimedia is not supported for the db.t3.micro or db.t3.small DB instance classes. For more information, see [RDS for Oracle instance classes \(p. 1477\)](#).
- Your DB instance must have **Auto Minor Version Upgrade** enabled. This option enables your DB instance to receive minor DB engine version upgrades automatically when they become available and is required for any options that install the Oracle Java Virtual Machine (JVM). Amazon RDS uses this option to update your DB instance to the latest Oracle Patch Set Update (PSU) or Release Update (RU). For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Best practices for Oracle Multimedia

The following are best practices for using Oracle Multimedia:

- For maximum security, use the MULTIMEDIA option with Secure Sockets Layer (SSL). For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).
- Configure your DB instance to restrict access to your DB instance. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#) and [Working with a DB instance in a VPC \(p. 2103\)](#).

Adding the Oracle Multimedia option

The following is the general process for adding the MULTIMEDIA option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the MULTIMEDIA option is added. There is no outage if Oracle Java Virtual Machine (JVM) is already installed

on the DB instance. After you add the option, you don't need to restart your DB instance. As soon as the option group is active, Oracle Multimedia is available.

Note

During this outage, password verification functions are disabled briefly. You can also expect to see events related to password verification functions during the outage. Password verification functions are enabled again before the Oracle DB instance is available.

To add the MULTIMEDIA option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose the edition for your Oracle DB instance.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).
2. Add the **MULTIMEDIA** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Removing the Oracle Multimedia option

After you drop all objects that use data types provided by the MULTIMEDIA option, you can remove the option from a DB instance. If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the MULTIMEDIA option is removed. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you remove the MULTIMEDIA option, you don't need to restart your DB instance.

To drop the MULTIMEDIA option

1. Back up your data.

Warning

If the instance uses data types that were enabled as part of the option, and if you remove the MULTIMEDIA option, you can lose data. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

2. Check whether any existing objects reference data types or features of the MULTIMEDIA option.
3. Drop any objects that reference data types or features of the MULTIMEDIA option.
4. Do one of the following:
 - Remove the MULTIMEDIA option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
 - Modify the DB instance and specify a different option group that doesn't include the MULTIMEDIA option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle native network encryption

Amazon RDS supports Oracle native network encryption (NNE). With native network encryption, you can encrypt data as it moves to and from a DB instance. Amazon RDS supports NNE for all editions of Oracle Database.

A detailed discussion of Oracle native network encryption is beyond the scope of this guide, but you should understand the strengths and weaknesses of each algorithm and key before you decide on a solution for your deployment. For information about the algorithms and keys that are available through Oracle native network encryption, see [Configuring network data encryption](#) in the Oracle documentation. For more information about AWS security, see the [AWS security center](#).

Note

You can use Native Network Encryption or Secure Sockets Layer, but not both. For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).

NNE option settings

You can specify encryption requirements on both the server and the client. The DB instance can act as a client when, for example, it uses a database link to connect to another database. You might want to avoid forcing encryption on the server side. For example, you might not want to force all client communications to use encryption because the server requires it. In this case, you can force encryption on the client side using the SQLNET.*CLIENT options.

Amazon RDS supports the following settings for the NNE option.

Note

When you use commas to separate values for an option setting, don't put a space after the comma.

Option setting	Valid values	Default values	Description
SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS	TRUE, FALSE	TRUE	<p>The behavior of the server when a client using a non-secure cipher attempts to connect to the database. If TRUE, clients can connect even if they aren't patched with the July 2021 PSU.</p> <p>If the setting is FALSE, clients can connect to the database only when they are patched with the July 2021 PSU. Before you set SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS to FALSE, make sure that the following conditions are met:</p> <ul style="list-style-type: none">SQLNET.ENCRYPTION_TYPES_SERVER and SQLNET.ENCRYPTION_TYPES_CLIENT have one matching encryption method that is not DES, 3DES, or RC4 (all key lengths).SQLNET.CHECKSUM_TYPES_SERVER and SQLNET.CHECKSUM_TYPES_CLIENT have one matching secure checksumming method that is not MD5.The client is patched with the July 2021 PSU. If the client isn't patched, the client loses the connection and receives the ORA-12269 error.

Option setting	Valid values	Default values	Description
SQLNET.ALLOW_WEAK_CRYPTO	TRUE, FALSE	TRUE	<p>The behavior of the server when a client using a non-secure cipher attempts to connect to the database. The following ciphers are considered not secure:</p> <ul style="list-style-type: none"> • DES encryption method (all key lengths) • 3DES encryption method (all key lengths) • RC4 encryption method (all key lengths) • MD5 checksumming method <p>If the setting is TRUE, clients can connect when they use the preceding non-secure ciphers.</p> <p>If the setting is FALSE, the database prevents clients from connecting when they use the preceding non-secure ciphers. Before you set SQLNET.ALLOW_WEAK_CRYPTO to FALSE, make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • SQLNET.ENCRYPTION_TYPES_SERVER and SQLNET.ENCRYPTION_TYPES_CLIENT have one matching encryption method that is not DES, 3DES, or RC4 (all key lengths). • SQLNET.CHECKSUM_TYPES_SERVER and SQLNET.CHECKSUM_TYPES_CLIENT have one matching secure checksumming method that is not MD5. • The client is patched with the July 2021 PSU. If the client isn't patched, the client loses the connection and receives the ORA-12269 error.
SQLNET.CRYPTO_CHECKSUM_CLIENT	Accepted, Rejected, Requested, Required	Requested	<p>The data integrity behavior when a DB instance connects to the client, or a server acting as a client. When a DB instance uses a database link, it acts as a client.</p> <p>Requested indicates that the client doesn't require the DB instance to perform a checksum.</p>
SQLNET.CRYPTO_CHECKSUM_SERVER	Accepted, Rejected, Requested, Required	Requested	<p>The data integrity behavior when a client, or a server acting as a client, connects to the DB instance. When a DB instance uses a database link, it acts as a client.</p> <p>Requested indicates that the DB instance doesn't require the client to perform a checksum.</p>

Option setting	Valid values	Default values	Description
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	SHA256, SHA384, SHA512, SHA1, MD5	SHA256, SHA384, SHA512	A list of checksum algorithms. You can specify either one value or a comma-separated list of values. If you use a comma, don't insert a space after the comma; otherwise, you receive an <code>InvalidParameterValue</code> error. This parameter and <code>SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER</code> must have a common cipher.
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	SHA256, SHA384, SHA512, SHA1, MD5	SHA256, SHA384, SHA512, SHA1, MD5	A list of checksum algorithms. You can specify either one value or a comma-separated list of values. If you use a comma, don't insert a space after the comma; otherwise, you receive an <code>InvalidParameterValue</code> error. This parameter and <code>SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT</code> must have a common cipher.
SQLNET.ENCRYPTION_CLIENT	Accepted, Rejected, Requested, Required	Requested	The encryption behavior of the client when a client, or a server acting as a client, connects to the DB instance. When a DB instance uses a database link, it acts as a client. Requested indicates that the client does not require traffic from the server to be encrypted.
SQLNET.ENCRYPTION_SERVER	Accepted, Rejected, Requested, Required	Requested	The encryption behavior of the server when a client, or a server acting as a client, connects to the DB instance. When a DB instance uses a database link, it acts as a client. Requested indicates that the DB instance does not require traffic from the client to be encrypted.

Option setting	Valid values	Default values	Description
SQLNET.ENCRYPTION_TYPES_CLIENT	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	<p>A list of encryption algorithms used by the client. The client uses each algorithm, in order, to attempt to decrypt the server input until an algorithm succeeds or until the end of the list is reached.</p> <p>Amazon RDS uses the following default list from Oracle. You can change the order or limit the algorithms that the DB instance will accept.</p> <ul style="list-style-type: none"> 1. RC4_256: RSA RC4 (256-bit key size) 2. AES256: AES (256-bit key size) 3. AES192: AES (192-bit key size) 4. 3DES168: 3-key Triple-DES (112-bit effective key size) 5. RC4_128: RSA RC4 (128-bit key size) 6. AES128: AES (128-bit key size) 7. 3DES112: 2-key Triple-DES (80-bit effective key size) 8. RC4_56: RSA RC4 (56-bit key size) 9. DES: Standard DES (56-bit key size) 10. RC4_40: RSA RC4 (40-bit key size) 11. DES40: DES40 (40-bit key size) <p>You can specify either one value or a comma-separated list of values. If you a comma, don't insert a space after the comma; otherwise, you receive an <code>InvalidParameterValue</code> error.</p> <p>This parameter and <code>SQLNET.SQLNET.ENCRYPTION_TYPES_SERVER</code> must have a common cipher.</p>

Option setting	Valid values	Default values	Description
SQLNET.ENCRYPTION_TYPES_SERVER	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	<p>A list of encryption algorithms used by the DB instance. The DB instance uses each algorithm, in order, to attempt to decrypt the client input until an algorithm succeeds or until the end of the list is reached.</p> <p>Amazon RDS uses the following default list from Oracle. You can change the order or limit the algorithms that the client will accept.</p> <ol style="list-style-type: none"> 1. RC4_256: RSA RC4 (256-bit key size) 2. AES256: AES (256-bit key size) 3. AES192: AES (192-bit key size) 4. 3DES168: 3-key Triple-DES (112-bit effective key size) 5. RC4_128: RSA RC4 (128-bit key size) 6. AES128: AES (128-bit key size) 7. 3DES112: 2-key Triple-DES (80-bit effective key size) 8. RC4_56: RSA RC4 (56-bit key size) 9. DES: Standard DES (56-bit key size) 10. RC4_40: RSA RC4 (40-bit key size) 11. DES40: DES40 (40-bit key size) <p>You can specify either one value or a comma-separated list of values. If you a comma, don't insert a space after the comma; otherwise, you receive an <code>InvalidParameterValue</code> error.</p> <p>This parameter and <code>SQLNET.SQLNET.ENCRYPTION_TYPES_SERVER</code> must have a common cipher.</p>

Adding the NNE option

The general process for adding the NNE option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

When the option group is active, NNE is active.

To add the NNE option to a DB instance using the AWS Management Console

1. For **Engine**, choose the Oracle edition that you want to use. NNE is supported on all editions.
2. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

3. Add the **NNE** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).

Note

After you add the NNE option, you don't need to restart your DB instances. As soon as the option group is active, NNE is active.

4. Apply the option group to a new or existing DB instance:

- For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. After you add the NNE option, you don't need to restart your DB instance. As soon as the option group is active, NNE is active. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Setting NNE values in the sqlnet.ora

With Oracle native network encryption, you can set network encryption on the server side and client side. The client is the computer used to connect to the DB instance. You can specify the following client settings in the sqlnet.ora:

- SQLNET.ALLOW_WEAK_CRYPTO
- SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS
- SQLNET.CRYPTO_CHECKSUM_CLIENT
- SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
- SQLNET.ENCRYPTION_CLIENT
- SQLNET.ENCRYPTION_TYPES_CLIENT

For information, see [Configuring network data encryption and integrity for Oracle servers and clients](#) in the Oracle documentation.

Sometimes, the DB instance rejects a connection request from an application. For example, a rejection can occur when the encryption algorithms on the client and on the server don't match. To test Oracle native network encryption, add the following lines to the sqlnet.ora file on the client:

```
DIAG_ADR_ENABLED=off
TRACE_DIRECTORY_CLIENT=/tmp
TRACE_FILE_CLIENT=nettrace
TRACE_LEVEL_CLIENT=16
```

When a connection is attempted, the preceding lines generate a trace file on the client called /tmp/nettrace*. The trace file contains information about the connection. For more information about connection-related issues when you are using Oracle Native Network Encryption, see [About negotiating encryption and integrity](#) in the Oracle Database documentation.

Modifying NNE option settings

After you enable NNE, you can modify settings for the option. For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [NNE option settings \(p. 1711\)](#).

Topics

- [Modifying CRYPTO_CHECKSUM_* values \(p. 1717\)](#)
- [Modifying ALLOW_WEAK_CRYPTO* settings \(p. 1717\)](#)

Modifying CRYPTO_CHECKSUM_* values

If you modify NNE option settings, make sure that the following option settings have at least one common cipher:

- SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER
- SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT

The following example shows a scenario in which you modify SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER. The configuration is valid because the CRYPTO_CHECKSUM_TYPES_CLIENT and CRYPTO_CHECKSUM_TYPES_SERVER both use SHA256.

Option setting	Values before modification	Values after modification
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	SHA256, SHA384, SHA512	No change
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	SHA256, SHA384, SHA512, SHA1, MD5	SHA1, MD5, SHA256

For another example, assume that you want to modify SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER from its default setting to SHA1, MD5. In this case, make sure you set SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT to SHA1 or MD5. These algorithms aren't included in the default values for SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT.

Modifying ALLOW_WEAK_CRYPTO* settings

To set the SQLNET.ALLOW_WEAK_CRYPTO* options from the default value to FALSE, make sure that the following conditions are met:

- SQLNET.ENCRYPTION_TYPES_SERVER and SQLNET.ENCRYPTION_TYPES_CLIENT have one matching secure encryption method. A method is considered secure if it's not DES, 3DES, or RC4 (all key lengths).
- SQLNET.CHECKSUM_TYPES_SERVER and SQLNET.CHECKSUM_TYPES_CLIENT have one matching secure checksumming method. A method is considered secure if it's not MD5.
- The client is patched with the July 2021 PSU. If the client isn't patched, the client loses the connection and receives the ORA-12269 error.

The following example shows sample NNE settings. Assume that you want to set SQLNET.ENCRYPTION_TYPES_SERVER and SQLNET.ENCRYPTION_TYPES_CLIENT to FALSE, thereby blocking non-secure connections. The checksum option settings meet the prerequisites because they both have SHA256. However, SQLNET.ENCRYPTION_TYPES_CLIENT and SQLNET.ENCRYPTION_TYPES_SERVER use the DES, 3DES, and RC4 encryption methods, which are non-secure. Therefore, to set the SQLNET.ALLOW_WEAK_CRYPTO* options to FALSE, first set SQLNET.ENCRYPTION_TYPES_SERVER and SQLNET.ENCRYPTION_TYPES_CLIENT to a secure encryption method such as AES256.

Option setting	Values
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	SHA256, SHA384, SHA512
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	SHA1, MD5, SHA256
SQLNET.ENCRYPTION_TYPES_CLIENT	RC4_256, 3DES168, DES40

Option setting	Values
SQLNET.ENCRYPTION_TYPES_SERVER	RC4_256, 3DES168, DES40

Removing the NNE option

You can remove NNE from a DB instance.

To remove NNE from a DB instance, do one of the following:

- To remove NNE from multiple DB instances, remove the NNE option from the option group they belong to. This change affects all DB instances that use the option group. After you remove the NNE option, you don't need to restart your DB instances. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove NNE from a single DB instance, modify the DB instance and specify a different option group that doesn't include the NNE option. You can specify the default (empty) option group, or a different custom option group. After you remove the NNE option, you don't need to restart your DB instance. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle OLAP

Amazon RDS supports Oracle OLAP through the use of the OLAP option. This option provides On-line Analytical Processing (OLAP) for Oracle DB instances. You can use Oracle OLAP to analyze large amounts of data by creating dimensional objects and cubes in accordance with the OLAP standard. For more information, see [the Oracle documentation](#).

Important

If you use Oracle OLAP, Amazon RDS automatically updates your DB instance to the latest Oracle PSU if there are security vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9+ or other announced security vulnerabilities.

Amazon RDS supports Oracle OLAP for the following editions and versions of Oracle:

- Oracle Database 21c Enterprise Edition, all versions
- Oracle Database 19c Enterprise Edition, all versions
- Oracle Database 12c Release 2 (12.2.0.1) Enterprise Edition, all versions
- Oracle Database 12c Release 1 (12.1.0.2) Enterprise Edition, version 12.1.0.2.v13 or later

Prerequisites for Oracle OLAP

The following are prerequisites for using Oracle OLAP:

- You must have an Oracle OLAP license from Oracle. For more information, see [Licensing Information](#) in the Oracle documentation.
- Your DB instance must be of a sufficient instance class. Oracle OLAP isn't supported for the db.t3.micro or db.t3.small DB instance classes. For more information, see [RDS for Oracle instance classes \(p. 1477\)](#).
- Your DB instance must have **Auto Minor Version Upgrade** enabled. This option enables your DB instance to receive minor DB engine version upgrades automatically when they become available and is required for any options that install the Oracle Java Virtual Machine (JVM). Amazon RDS uses this option to update your DB instance to the latest Oracle Patch Set Update (PSU) or Release Update (RU). For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- Your DB instance must not have a user named OLAPSYS. If it does, the OLAP option installation fails.

Best practices for Oracle OLAP

The following are best practices for using Oracle OLAP:

- For maximum security, use the OLAP option with Secure Sockets Layer (SSL). For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).
- Configure your DB instance to restrict access to your DB instance. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#) and [Working with a DB instance in a VPC \(p. 2103\)](#).

Adding the Oracle OLAP option

The following is the general process for adding the OLAP option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the OLAP option is added. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you add the option, you don't need to restart your DB instance. As soon as the option group is active, Oracle OLAP is available.

To add the OLAP option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - For **Engine**, choose the Oracle edition for your DB instance.
 - For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **OLAP** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Using Oracle OLAP

After you enable the Oracle OLAP option, you can begin using it. For a list of features that are supported for Oracle OLAP, see [the Oracle documentation](#).

Removing the Oracle OLAP option

After you drop all objects that use data types provided by the OLAP option, you can remove the option from a DB instance. If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the OLAP option is removed. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you remove the OLAP option, you don't need to restart your DB instance.

To drop the OLAP option

1. Back up your data.

Warning

If the instance uses data types that were enabled as part of the option, and if you remove the OLAP option, you can lose data. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

2. Check whether any existing objects reference data types or features of the OLAP option.
3. Drop any objects that reference data types or features of the OLAP option.
4. Do one of the following:
 - Remove the OLAP option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
 - Modify the DB instance and specify a different option group that doesn't include the OLAP option. This change affects a single DB instance. You can specify the default (empty) option group,

or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Secure Sockets Layer

You enable Secure Sockets Layer (SSL) encryption for an Oracle DB instance by adding the Oracle SSL option to the option group associated with an Oracle DB instance. You specify the port you want to communicate over using SSL. You must configure SQL*Plus as shown in this following section.

You enable SSL encryption for an Oracle DB instance by adding the Oracle SSL option to the option group associated with the DB instance. Amazon RDS uses a second port, as required by Oracle, for SSL connections. This approach allows both clear text and SSL-encrypted communication to occur at the same time between a DB instance and SQL*Plus. For example, you can use the port with clear text communication to communicate with other resources inside a VPC while using the port with SSL-encrypted communication to communicate with resources outside the VPC.

Note

You can use Secure Sockets Layer or Native Network Encryption, but not both. For more information, see [Oracle native network encryption \(p. 1711\)](#).

You can use SSL encryption with all editions of the following Oracle database versions:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)
- Oracle Database 12c Release 2 (12.2)
- Oracle Database 12c Release 1 (12.1)

Note

You cannot use both SSL and Oracle native network encryption (NNE) on the same instance. If you use SSL encryption, you must disable any other connection encryption.

TLS versions for the Oracle SSL option

Amazon RDS for Oracle supports Transport Layer Security (TLS) versions 1.0 and 1.2. To use the Oracle SSL option, use the SQLNET.SSL_VERSION option setting. The following values are allowed for this option setting:

- "1.0" – Clients can connect to the DB instance using TLS 1.0 only.
- "1.2" – Clients can connect to the DB instance using TLS 1.2 only.
- "1.2 or 1.0" – Clients can connect to the DB instance using either TLS 1.2 or 1.0.

To use the Oracle SSL option, the SQLNET.SSL_VERSION option setting is also required:

- For existing Oracle SSL options, SQLNET.SSL_VERSION is set to "1.0" automatically. You can change the setting if necessary.
- When you add a new Oracle SSL option, you must set SQLNET.SSL_VERSION explicitly to a valid value.

The following table shows the TLS option settings that are supported for different Oracle engine versions and editions.

Oracle engine version	SQLNET.SSL_VERSION = "1.0"	SQLNET.SSL_VERSION = "1.2"	SQLNET.SSL_VERSION = "1.2 or 1.0"
21.0.0.0 (All editions)	Supported	Supported	Supported
19.0.0.0 (All editions)	Supported	Supported	Supported

Oracle engine version	<code>SQLNET.SSL_VERSION = "1.0"</code>	<code>SQLNET.SSL_VERSION = "1.2"</code>	<code>SQLNET.SSL_VERSION = "1.2 or 1.0"</code>
12.2.0.1 (All editions)	Supported	Supported	Supported
12.1.0.2 (All editions)	Supported	Supported	Supported

Cipher suites for the Oracle SSL option

Amazon RDS for Oracle supports multiple SSL cipher suites. By default, the Oracle SSL option is configured to use the `SSL_RSA_WITH_AES_256_CBC_SHA` cipher suite. To specify a different cipher suite to use over SSL connections, use the `SQLNET.CIPHER_SUITE` option setting. Following are the allowed values for this option setting:

- "`SSL_RSA_WITH_AES_256_CBC_SHA`" – The default setting, which is compatible with TLS 1.0 and TLS 1.2
- "`SSL_RSA_WITH_AES_256_CBC_SHA256`" – Only compatible with TLS 1.2
- "`SSL_RSA_WITH_AES_256_GCM_SHA384`" – Only compatible with TLS 1.2

For existing Oracle SSL options, `SQLNET.CIPHER_SUITE` is set to `"SSL_RSA_WITH_AES_256_CBC_SHA"` automatically. You can change the setting if necessary.

The following table shows the cipher suite option settings that are supported for different Oracle engine versions and editions.

Oracle engine version	<code>SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_256_GCM_SHA256"</code>	<code>SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_256_CBC_SHA256"</code>	<code>SQLNET.CIPHER_SUITE = "SSL_RSA_WITH_AES_256_CBC_SHA"</code>
19.0.0.0 (All editions)	Supported	Supported	Supported
12.2.0.1 (All editions)	Supported	Supported	Supported
12.1.0.2 (All editions)	Supported	Supported	Supported

FIPS support

Amazon RDS for Oracle enables you to use the Federal Information Processing Standard (FIPS) standard for 140-2. FIPS 140-2 is a United States government standard that defines cryptographic module security requirements. You enable the FIPS standard by setting the setting `FIPS.SSLFIPS_140` to `TRUE` for the Oracle SSL option. When FIPS 140-2 is configured for SSL, the cryptographic libraries are designed to encrypt data between the client and the Oracle DB instance.

You can enable the FIPS setting with the following Oracle database versions and editions:

- 19.0.0.0: All versions, all editions including Standard Edition Two
- 12.2.0.1: All versions, all editions including Standard Edition Two
- 12.1.0.2: Version 2 and later, all editions including Standard Edition Two

Clients must use the cipher suite that is FIPS-compliant. When establishing a connection, the client and Oracle DB instance negotiate which cipher suite to use when transmitting messages back and forth. The following table shows the FIPS-compliant SSL cipher suites for each TLS version.

SQLNET.SSL_VERSION	Supported cipher suites
1.0	SSL_RSA_WITH_AES_256_CBC_SHA
1.2	SSL_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_AES_256_GCM_SHA384

For more information, see [Oracle database FIPS 140-2 settings](#) in the Oracle documentation.

Adding the SSL option

To use SSL, your Amazon RDS for Oracle DB instance must be associated with an option group that includes the SSL option.

Console

To add the SSL option to an option group

1. Create a new option group or identify an existing option group to which you can add the SSL option.
For information about creating an option group, see [Creating an option group \(p. 274\)](#).
2. Add the SSL option to the option group.

If you want to use only FIPS-verified cipher suites for SSL connections, set the option `FIPS.SSLFIPS_140` to TRUE. For information about the FIPS standard, see [FIPS support \(p. 1723\)](#).

For information about adding an option to an option group, see [Adding an option to an option group \(p. 277\)](#).

3. Create a new Oracle DB instance and associate the option group with it, or modify an Oracle DB instance to associate the option group with it.

For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

To add the SSL option to an option group

1. Create a new option group or identify an existing option group to which you can add the SSL option.
For information about creating an option group, see [Creating an option group \(p. 274\)](#).
2. Add the SSL option to the option group.

Specify the following option settings:

- `Port` – The SSL port number
- `VpcSecurityGroupMemberships` – The VPC security group for which the option is enabled
- `SQLNET.SSL_VERSION` – The TLS version that client can use to connect to the DB instance

For example, the following AWS CLI command adds the SSL option to an option group named `ora-option-group`.

Example

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group --option-group-name ora-option-group \
    --options
    'OptionName=SSL,Port=2484,VpcSecurityGroupMemberships="sg-68184619",OptionSettings=[{Name=SQLNET.SSL...]
```

For Windows:

```
aws rds add-option-to-option-group --option-group-name ora-option-group ^
    --options
    'OptionName=SSL,Port=2484,VpcSecurityGroupMemberships="sg-68184619",OptionSettings=[{Name=SQLNET.SSL...]
```

3. Create a new Oracle DB instance and associate the option group with it, or modify an Oracle DB instance to associate the option group with it.

For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Configuring SQL*Plus to use SSL with an Oracle DB instance

You must configure SQL*Plus before connecting to an Oracle DB instance that uses the Oracle SSL option.

Note

To allow access to the DB instance from the appropriate clients, ensure that your security groups are configured correctly. For more information, see [Controlling access with security groups \(p. 2085\)](#). Also, these instructions are for SQL*Plus and other clients that directly use an Oracle home. For JDBC connections, see [Setting up an SSL connection over JDBC \(p. 1727\)](#).

To configure SQL*Plus to use SSL to connect to an Oracle DB instance

1. Set the ORACLE_HOME environment variable to the location of your Oracle home directory.

The path to your Oracle home directory depends on your installation. The following example sets the ORACLE_HOME environment variable.

```
prompt>export ORACLE_HOME=/home/user/app/user/product/12.1.0/dbhome_1
```

For information about setting Oracle environment variables, see [SQL*Plus environment variables](#) in the Oracle documentation, and also see the Oracle installation guide for your operating system.

2. Append \$ORACLE_HOME/lib to the LD_LIBRARY_PATH environment variable.

The following is an example that sets the LD_LIBRARY_PATH environment variable.

```
prompt>export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
```

3. Create a directory for the Oracle wallet at \$ORACLE_HOME/ssl_wallet.

The following is an example that creates the Oracle wallet directory.

```
prompt>mkdir $ORACLE_HOME/ssl_wallet
```

4. Download the root certificate that works for all AWS Regions and put the file in the ssl_wallet directory.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

5. In the \$ORACLE_HOME/network/admin directory, modify or create the tnsnames.ora file and include the following entry.

```
<net_service_name>= (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)
    (HOST = <endpoint>) (PORT = <ssl port number>)))(CONNECT_DATA = (SID = <database
    name>))
    (SECURITY = (SSL_SERVER_CERT_DN =
    "C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,CN=<endpoint>")))
```

6. In the same directory, modify or create the sqlnet.ora file and include the following parameters.

Note

To communicate with entities over a TLS secured connection, Oracle requires a wallet with the necessary certificates for authentication. You can use Oracle's ORAPKI utility to create and maintain Oracle wallets, as shown in step 7. For more information, see [Setting up Oracle wallet using ORAPKI](#) in the Oracle documentation.

```
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY = $ORACLE_HOME/
ssl_wallet)))
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 1.0
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA)
SSL_SERVER_DN_MATCH = ON
```

Note

You can set SSL_VERSION to a higher value if your DB instance supports it.

7. Run the following commands to create the Oracle wallet.

```
prompt>orapki wallet create -wallet $ORACLE_HOME/ssl_wallet -auto_login_only
prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert
$ORACLE_HOME/ssl_wallet/rds-ca-2019-root.pem -auto_login_only
```

Replace the file name with the one you downloaded.

Connecting to an Oracle DB instance using SSL

After you configure SQL*Plus to use SSL as described previously, you can connect to the Oracle DB instance with the SSL option. Optionally, you can first export the TNS_ADMIN value that points to the directory that contains the tnsnames.ora and sqlnet.ora files. Doing so ensures that SQL*Plus can find these files consistently. The following example exports the TNS_ADMIN value.

```
export TNS_ADMIN = ${ORACLE_HOME}/network/admin
```

Connect to the DB instance. For example, you can connect using SQL*Plus and a *<net_service_name>* in a tnsnames.ora file.

```
sqlplus <mydbuser>@<net_service_name>
```

You can also connect to the DB instance using SQL*Plus without using a tnsnames.ora file by using the following command.

```
sqlplus '<mydbuser>@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST = <endpoint>) (PORT = <ssl port number>))(CONNECT_DATA = (SID = <database name>)))'
```

You can also connect to the Oracle DB instance without using SSL. For example, the following command connects to the DB instance through the clear text port without SSL encryption.

```
sqlplus '<mydbuser>@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = <endpoint>) (PORT = <port number>))(CONNECT_DATA = (SID = <database name>)))'
```

If you want to close Transmission Control Protocol (TCP) port access, create a security group with no IP address ingresses and add it to the instance. This addition closes connections over the TCP port, while still allowing connections over the SSL port that are specified from IP addresses within the range permitted by the SSL option security group.

Setting up an SSL connection over JDBC

To use an SSL connection over JDBC, you must create a keystore, trust the Amazon RDS root CA certificate, and use the code snippet specified following.

To create the keystore in JKS format, use the following command. For more information about creating the keystore, see the [Oracle documentation](#).

```
keytool -keystore clientkeystore -genkey -alias client
```

Next, take the following steps to trust the Amazon RDS root CA certificate.

To trust the Amazon RDS root CA certificate

1. Download the root certificate that works for all AWS Regions and put the file in the ssl_wallet directory.

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

2. Convert the certificate to .der format using the following command.

```
openssl x509 -outform der -in rds-ca-2019-root.pem -out rds-ca-2019-root.der
```

Replace the file name with the one you downloaded.

3. Import the certificate into the keystore using the following command.

```
keytool -import -alias rds-root -keystore clientkeystore.jks -file rds-ca-2019-root.der
```

4. Confirm that the key store was created successfully.

```
keytool -list -v -keystore clientkeystore.jks
```

Enter the keystore password when you are prompted for it.

The following code example shows how to set up the SSL connection using JDBC.

```

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.util.Properties;

public class OracleSslConnectionTest {
    private static final String DB_SERVER_NAME = "<dns-name-provided-by-amazon-rds>";
    private static final Integer SSL_PORT = "<ssl-option-port-configured-in-option-group>";
    private static final String DB_SID = "<oracle-sid>";
    private static final String DB_USER = "<user name>";
    private static final String DB_PASSWORD = "<password>";
    // This key store has only the prod root ca.
    private static final String KEY_STORE_FILE_PATH = "<file-path-to-keystore>";
    private static final String KEY_STORE_PASS = "<keystore-password>";

    public static void main(String[] args) throws SQLException {
        final Properties properties = new Properties();
        final String connectionString = String.format(
            "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=%d))" +
            "(CONNECT_DATA=(SID=%s)))",
            DB_SERVER_NAME, SSL_PORT, DB_SID);
        properties.put("user", DB_USER);
        properties.put("password", DB_PASSWORD);
        properties.put("oracle.jdbc.J2EE13Compliant", "true");
        properties.put("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        properties.put("javax.net.ssl.trustStoreType", "JKS");
        properties.put("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);
        final Connection connection = DriverManager.getConnection(connectionString,
        properties);
        // If no exception, that means handshake has passed, and an SSL connection can be
        opened
    }
}

```

Enforcing a DN match with an SSL connection

You can use the Oracle parameter SSL_SERVER_DN_MATCH to enforce that the distinguished name (DN) for the database server matches its service name. If you enforce the match verifications, then SSL ensures that the certificate is from the server. If you don't enforce the match verification, then SSL performs the check but allows the connection, regardless if there is a match. If you do not enforce the match, you allow the server to potentially fake its identify.

To enforce DN matching, add the DN match property and use the connection string specified below.

Add the property to the client connection to enforce DN matching.

```
properties.put("oracle.net.ssl_server_dn_match", "TRUE");
```

Use the following connection string to enforce DN matching when using SSL.

```

final String connectionString = String.format(
    "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=%d))" +
    "(CONNECT_DATA=(SID=%s))" +
    "(SECURITY = (SSL_SERVER_CERT_DN =
    \"C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,CN=%s\")))",

```

```
DB_SERVER_NAME, SSL_PORT, DB_SID, DB_SERVER_NAME);
```

Oracle Spatial

Amazon RDS supports Oracle Spatial through the use of the SPATIAL option. Oracle Spatial provides a SQL schema and functions that facilitate the storage, retrieval, update, and query of collections of spatial data in an Oracle database. For more information, see [Spatial Concepts](#) in the Oracle documentation.

Important

If you use Oracle Spatial, Amazon RDS automatically updates your DB instance to the latest Oracle PSU when any of the following exist:

- Security vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 9+
- Other announced security vulnerabilities

Amazon RDS supports Oracle Spatial only in Oracle Enterprise Edition (EE) and Oracle Standard Edition 2 (SE2). The following table shows the versions of the DB engine that support EE and SE2.

Oracle DB Version	EE	SE2
21.0.0.0, all versions	Yes	Yes
19.0.0.0, all versions	Yes	Yes
12.2.0.1, all versions	Yes	Yes
12.1.0.2.v13 or later	Yes	No

Prerequisites for Oracle Spatial

The following are prerequisites for using Oracle Spatial:

- Make sure that your DB instance is of a sufficient instance class. Oracle Spatial isn't supported for the db.t3.micro or db.t3.small DB instance classes. For more information, see [RDS for Oracle instance classes \(p. 1477\)](#).
- Make sure that your DB instance has **Auto Minor Version Upgrade** enabled. This option enables your DB instance to receive minor DB engine version upgrades automatically when they become available and is required for any options that install the Oracle Java Virtual Machine (JVM). Amazon RDS uses this option to update your DB instance to the latest Oracle Patch Set Update (PSU) or Release Update (RU). For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Best practices for Oracle Spatial

The following are best practices for using Oracle Spatial:

- For maximum security, use the SPATIAL option with Secure Sockets Layer (SSL). For more information, see [Oracle Secure Sockets Layer \(p. 1722\)](#).
- Configure your DB instance to restrict access to your DB instance. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#) and [Working with a DB instance in a VPC \(p. 2103\)](#).

Adding the Oracle Spatial option

The following is the general process for adding the SPATIAL option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the SPATIAL option is added. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you add the option, you don't need to restart your DB instance. As soon as the option group is active, Oracle Spatial is available.

Note

During this outage, password verification functions are disabled briefly. You can also expect to see events related to password verification functions during the outage. Password verification functions are enabled again before the Oracle DB instance is available.

To add the SPATIAL option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose the Oracle edition for your DB instance.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).
2. Add the **SPATIAL** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Removing the Oracle Spatial option

After you drop all objects that use data types provided by the SPATIAL option, you can drop the option from a DB instance. If Oracle Java Virtual Machine (JVM) is *not* installed on the DB instance, there is a brief outage while the SPATIAL option is removed. There is no outage if Oracle Java Virtual Machine (JVM) is already installed on the DB instance. After you remove the SPATIAL option, you don't need to restart your DB instance.

To drop the SPATIAL option

1. Back up your data.

Warning

If the instance uses data types that were enabled as part of the option, and if you remove the SPATIAL option, you can lose data. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

2. Check whether any existing objects reference data types or features of the SPATIAL option.

If SPATIAL options exist, the instance can get stuck when applying the new option group that doesn't have the SPATIAL option. You can identify the objects by using the following queries:

```
SELECT OWNER, SEGMENT_NAME, TABLESPACE_NAME, BYTES/1024/1024 mbytes
```

```
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE '%TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
       (SELECT DISTINCT OWNER, TABLE_NAME
        FROM   DBA_TAB_COLUMNS
        WHERE  DATA_TYPE='SDO_GEOGRAPHY'
        AND    OWNER <> 'MDSYS')
ORDER BY 1,2,3,4;

SELECT OWNER, TABLE_NAME, COLUMN_NAME
FROM   DBA_TAB_COLUMNS
WHERE  DATA_TYPE = 'SDO_GEOGRAPHY'
AND    OWNER <> 'MDSYS'
ORDER BY 1,2,3;
```

3. Drop any objects that reference data types or features of the SPATIAL option.
4. Do one of the following:
 - Remove the SPATIAL option from the option group it belongs to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
 - Modify the DB instance and specify a different option group that doesn't include the SPATIAL option. This change affects a single DB instance. You can specify the default (empty) option group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle SQLT

Amazon RDS supports Oracle SQLTXPLAIN (SQLT) through the use of the SQLT option.

The Oracle EXPLAIN PLAN statement can determine the execution plan of a SQL statement. It can verify whether the Oracle optimizer chooses a certain execution plan, such as a nested loops join. It also helps you understand the optimizer's decisions, such as why it chose a nested loops join over a hash join. So EXPLAIN PLAN helps you understand the statement's performance.

SQLT is an Oracle utility that produces a report. The report includes object statistics, object metadata, optimizer-related initialization parameters, and other information that a database administrator can use to tune a SQL statement for optimal performance. SQLT produces an HTML report with hyperlinks to all of the sections in the report.

Unlike Automatic Workload Repository or Statspack reports, SQLT works on individual SQL statements. SQLT is a collection of SQL, PL/SQL, and SQL*Plus files that collect, store, and display performance data.

Following are the supported Oracle versions for each SQLT version.

SQLT version	Oracle Database 21c	Oracle Database 19c	Oracle Database 12c Release 2 (12.2)	Oracle Database 12c Release 1 (12.1)
2018-07-25.v1	Supported	Supported	Supported	Supported
2018-03-31.v1	Not supported	Not supported	Supported	Supported
2016-04-29.v1	Not supported	Not supported	Supported	Supported

To download SQLT and access instructions for using it:

- Log in to your My Oracle Support account, and open the following documents:
 - To download SQLT: [Document 215187.1](#)
 - For SQLT usage instructions: [Document 1614107.1](#)
 - For frequently asked questions about SQLT: [Document 1454160.1](#)
 - For information about reading SQLT output: [Document 1456176.1](#)
 - For interpreting the Main report: [Document 1922234.1](#)

You can use SQLT with any edition of the following Oracle Database versions:

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c Release 2 (12.2.0.1)
- Oracle Database 12c Release 1 (12.1.0.2)

Amazon RDS does not support the following SQLT methods:

- XPORE
- XHUME

Prerequisites for SQLT

The following are prerequisites for using SQLT:

- You must remove users and roles that are required by SQLT, if they exist.

The SQLT option creates the following users and roles on a DB instance:

- SQLTXPLAIN user
- SQLTXADMIN user
- SQLT_USER_ROLE role

If your DB instance has any of these users or roles, log in to the DB instance using a SQL client, and drop them using the following statements:

```
DROP USER SQLTXPLAIN CASCADE;
DROP USER SQLTXADMIN CASCADE;
DROP ROLE SQLT_USER_ROLE CASCADE;
```

- You must remove tablespaces that are required by SQLT, if they exist.

The SQLT option creates the following tablespaces on a DB instance:

- RDS_SQLT_TS
- RDS_TEMP_SQLT_TS

If your DB instance has these tablespaces, log in to the DB instance using a SQL client, and drop them.

SQL option settings

SQLT can work with licensed features that are provided by the Oracle Tuning Pack and the Oracle Diagnostics Pack. The Oracle Tuning Pack includes the SQL Tuning Advisor, and the Oracle Diagnostics Pack includes the Automatic Workload Repository. The SQLT settings enable or disable access to these features from SQLT.

Amazon RDS supports the following settings for the SQLT option.

Option setting	Valid values	Default value	Description
LICENSE_PACK	T, D, N	N	<p>The Oracle Management Packs that you want to access with SQLT. Enter one of the following values:</p> <ul style="list-style-type: none"> • T indicates that you have a license for the Oracle Tuning Pack and the Oracle Diagnostics Pack, and you want to access the SQL Tuning Advisor and Automatic Workload Repository from SQLT. • D indicates that you have a license for the Oracle Diagnostics Pack, and you want to access the Automatic Workload Repository from SQLT. • N indicates that you don't have a license for the Oracle Tuning Pack and the Oracle Diagnostics Pack, or that you have a license for one or both of them, but you don't want SQLT to access them.

Option setting	Valid values	Default value	Description
			<p>Note Amazon RDS does not provide licenses for these Oracle Management Packs. If you indicate that you want to use a pack that is not included in your DB instance, you can use SQLT with the DB instance. However, SQLT can't access the pack, and the SQLT report doesn't include the data for the pack. For example, if you specify T, but the DB instance doesn't include the Oracle Tuning Pack, SQLT works on the DB instance, but the report it generates doesn't contain data related to the Oracle Tuning Pack.</p>
VERSION	2016-04-29.v1 2018-03-31.v1 2018-07-25.v1	2016-04-29.v1	The version of SQLT that you want to install. <p>Note For Oracle Database 19c and 21c, the only supported version is 2018-07-25.v1. This version is the default for these releases. </p>

Adding the SQLT option

The following is the general process for adding the SQLT option to a DB instance:

1. Create a new option group, or copy or modify an existing option group.
2. Add the SQLT option to the option group.
3. Associate the option group with the DB instance.

After you add the SQLT option, as soon as the option group is active, SQLT is active.

To add the SQLT option to a DB instance

1. Determine the option group that you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine**, choose the Oracle edition that you want to use. The SQLT option is supported on all editions.
 - b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **SQLT** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

- For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
4. (Optional) Verify the SQLT installation on each DB instance with the SQLT option.

- a. Use a SQL client to connect to the DB instance as the master user.

For information about connecting to an Oracle DB instance using a SQL client, see [Connecting to your Oracle DB instance \(p. 1488\)](#).

- b. Run the following query:

```
SELECT sqlxplain.sqlt$a.get_param('tool_version') sqlt_version FROM DUAL;
```

The query returns the current version of the SQLT option on Amazon RDS. 12.1.160429 is an example of a version of SQLT that is available on Amazon RDS.

5. Change the passwords of the users that are created by the SQLT option.

- a. Use a SQL client to connect to the DB instance as the master user.

- b. Run the following SQL statement to change the password for the SQLTXADMIN user:

```
ALTER USER SQLTXADMIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

- c. Run the following SQL statement to change the password for the SQLXPLAIN user:

```
ALTER USER SQLXPLAIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

Note

Upgrading SQLT requires uninstalling an older version of SQLT and then installing the new version. So, all SQLT metadata can be lost when you upgrade SQLT. A major version upgrade of a database also uninstalls and re-installs SQLT. An example of a major version upgrade is an upgrade from Oracle Database 12c Release 2 (12.2) to Oracle Database 19c.

Using SQLT

SQLT works with the Oracle SQL*Plus utility.

To use SQLT

1. Download the SQLT .zip file from [Document 215187.1](#) on the My Oracle Support site.

Note

You can't download SQLT 12.1.160429 from the My Oracle Support site. Oracle has deprecated this older version.

2. Unzip the SQLT .zip file.
3. From a command prompt, change to the sqlt/run directory on your file system.
4. From the command prompt, open SQL*Plus, and connect to the DB instance as the master user.

For information about connecting to a DB instance using SQL*Plus, see [Connecting to your Oracle DB instance \(p. 1488\)](#).

5. Get the SQL ID of a SQL statement:

```
SELECT SQL_ID FROM V$SQL WHERE SQL_TEXT='sql_statement';
```

Your output is similar to the following:

```
SQL_ID
-----
chvsmttqjzjkn
```

6. Analyze a SQL statement with SQLT:

```
START sqltxtract.sql sql_id sqlxplain_user_password
```

For example, for the SQL ID chvsmttqjzjkn, enter the following:

```
START sqltxtract.sql chvsmttqjzjkn sqlxplain_user_password
```

SQLT generates the HTML report and related resources as a .zip file in the directory from which the SQLT command was run.

7. (Optional) To enable application users to diagnose SQL statements with SQLT, grant SQLT_USER_ROLE to each application user with the following statement:

```
GRANT SQLT_USER_ROLE TO application_user_name;
```

Note

Oracle does not recommend running SQLT with the SYS user or with users that have the DBA role. It is a best practice to run SQLT diagnostics using the application user's account, by granting SQLT_USER_ROLE to the application user.

Upgrading the SQLT option

With Amazon RDS for Oracle, you can upgrade the SQLT option from your existing version to a higher version. To upgrade the SQLT option, complete steps 1–3 in [Using SQLT \(p. 1736\)](#) for the new version of SQLT. Also, if you granted privileges for the previous version of SQLT in step 7 of that section, grant the privileges again for the new SQLT version.

Upgrading the SQLT option results in the loss of the older SQLT version's metadata. The older SQLT version's schema and related objects are dropped, and the newer version of SQLT is installed. For more information about the changes in the latest SQLT version, see [Document 1614201.1](#) on the My Oracle Support site.

Note

Version downgrades are not supported.

Modifying SQLT settings

After you enable SQLT, you can modify the LICENSE_PACK and VERSION settings for the option.

For more information about how to modify option settings, see [Modifying an option setting \(p. 282\)](#). For more information about each setting, see [SQLT option settings \(p. 1734\)](#).

Removing the SQLT option

You can remove SQLT from a DB instance.

To remove SQLT from a DB instance, do one of the following:

- To remove SQLT from multiple DB instances, remove the SQLT option from the option group to which the DB instances belong. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove SQLT from a single DB instance, modify the DB instance and specify a different option group that doesn't include the SQLT option. You can specify the default (empty) option group or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Oracle Statspack

The Oracle Statspack option installs and enables the Oracle Statspack performance statistics feature. Oracle Statspack is a collection of SQL, PL/SQL, and SQL*Plus scripts that collect, store, and display performance data. For information about using Oracle Statspack, see [Oracle Statspack](#) in the Oracle documentation.

Note

Oracle Statspack is no longer supported by Oracle and has been replaced by the more advanced Automatic Workload Repository (AWR). AWR is available only for Oracle Enterprise Edition customers who have purchased the Diagnostics Pack. You can use Oracle Statspack with any Oracle DB engine on Amazon RDS. You can't run Oracle Statspack on Amazon RDS read replicas.

Setting up Oracle Statspack

To run Statspack scripts, you must add the Statspack option.

To set up Oracle Statspack

1. In a SQL client, log in to the Oracle DB with an administrative account.
2. Do either of the following actions, depending on whether Statspack is installed:
 - If Statspack is installed, and the PERFSTAT account is associated with Statspack, skip to Step 4.
 - If Statspack is not installed, and the PERFSTAT account exists, drop the account as follows:

```
DROP USER PERFSTAT CASCADE;
```

Otherwise, attempting to add the Statspack option generates an error and RDS-Event-0058.

3. Add the Statspack option to an option group. See [Adding an option to an option group \(p. 277\)](#).

Amazon RDS automatically installs the Statspack scripts on the DB instance and then sets up the PERFSTAT account.

4. Reset the password using the following SQL statement, replacing *pwd* with your new password:

```
ALTER USER PERFSTAT IDENTIFIED BY pwd ACCOUNT UNLOCK;
```

You can log in using the PERFSTAT user account and run the Statspack scripts.

5. Do either of the following actions, depending on your DB engine version:

- If you are using Oracle Database 12c Release 2 (12.2) or lower, skip this step.
- If you are using Oracle Database 19c or higher, grant the CREATE JOB privilege to the PERFSTAT account using the following statement:

```
GRANT CREATE JOB TO PERFSTAT;
```

6. Ensure that idle wait events in the PERFSTAT.STATS\$IDLE_EVENT table are populated.

Because of Oracle Bug 28523746, the idle wait events in PERFSTAT.STATS\$IDLE_EVENT may not be populated. To ensure all idle events are available, run the following statement:

```
INSERT INTO PERFSTAT.STATS$IDLE_EVENT (EVENT)
SELECT NAME FROM V$EVENT_NAME WHERE WAIT_CLASS='Idle'
MINUS
SELECT EVENT FROM PERFSTAT.STATS$IDLE_EVENT;
```

```
COMMIT;
```

Generating Statspack reports

A Statspack report compares two snapshots.

To generate Statspack reports

1. In a SQL client, log in to the Oracle DB with the PERFSTAT account.
2. Create a snapshot using either of the following techniques:
 - Create a Statspack snapshot manually.
 - Create a job that takes a Statspack snapshot after a given time interval. For example, the following job creates a Statspack snapshot every hour:

```
VARIABLE jn NUMBER;
exec dbms_job.submit(:jn, 'statspack.snap;',SYSDATE,'TRUNC(SYSDATE+1/24, ''HH24'')");
COMMIT;
```

3. View the snapshots using the following query:

```
SELECT SNAP_ID, SNAP_TIME FROM STATS$SNAPSHOT ORDER BY 1;
```

4. Run the Amazon RDS procedure `rdsadmin.rds_run_sreport`, replacing `begin_snap` and `end_snap` with the snapshot IDs:

```
exec rdsadmin.rds_run_sreport(begin_snap,end_snap);
```

For example, the following command creates a report based on the interval between Statspack snapshots 1 and 2:

```
exec rdsadmin.rds_run_sreport(1,2);
```

The file name of the Statspack report includes the number of the two snapshots. For example, a report file created using Statspack snapshots 1 and 2 would be named ORCL_sreport_1_2.lst.

5. Monitor the output for errors.

Oracle Statspack performs checks before running the report. Therefore, you could also see error messages in the command output. For example, you might try to generate a report based on an invalid range, where the beginning Statspack snapshot value is larger than the ending value. In this case, the output shows the error message, but the DB engine does not generate an error file.

```
exec rdsadmin.rds_run_sreport(2,1);
*
ERROR at line 1:
ORA-20000: Invalid snapshot IDs. Find valid ones in perfstat.stats$snapshot.
```

If you use an invalid number a Statspack snapshot, the output shows an error. For example, if you try to generate a report for snapshots 1 and 50, but snapshot 50 doesn't exist, the output shows an error.

```
exec rdsadmin.rds_run_sreport(1,50);
*
ERROR at line 1:
```

ORA-20000: Could not find both snapshot IDs

6. (Optional)

To retrieve the report, call the trace file procedures, as explained in [Working with Oracle trace files \(p. 709\)](#).

Alternatively, download the Statspack report from the RDS console. Go to the **Log** section of the DB instance details and choose **Download**:

Logs (342)		
Name	Last written	Size
trace/ORCL_mmon_11800.trc	Thu Jan 18 09:39:14 GMT-800 2018	68.2 kB
trace/ORCL_mmon_11800.trm	Thu Jan 18 09:39:14 GMT-800 2018	6.7 kB
trace/ORCL_sreport_1_2.lst	Thu Jan 18 09:38:05 GMT-800 2018	107.5 kB
trace/alert_ORCL.log	Thu Jan 18 09:37:39 GMT-800 2018	60.5 kB
audit/ORCL ora_26710_20180118175137366624143795.aud	Thu Jan 18 09:31:57 GMT-800 2018	3.5 kB

If an error occurs while generating a report, the DB engine uses the same naming conventions as for a report but with an extension of .err. For example, if an error occurred while creating a report using Statspack snapshots 1 and 7, the report file would be named ORCL_sreport_1_7.err. You can download the error report using the same techniques as for a standard Snapshot report.

Removing Statspack files

To remove Oracle Statspack files, use the following command:

```
exec statspack.purge(begin snap, end snap);
```

Oracle time zone

To change the system time zone used by your Oracle DB instance, use the time zone option. For example, you might change the time zone of a DB instance to be compatible with an on-premises environment, or a legacy application. The time zone option changes the time zone at the host level. Changing the time zone impacts all date columns and values, including SYSDATE and SYSTIMESTAMP.

The time zone option differs from the `rdsadmin_util.alter_db_time_zone` command. The `alter_db_time_zone` command changes the time zone only for certain data types. The time zone option changes the time zone for all date columns and values. For more information about `alter_db_time_zone`, see [Setting the database time zone \(p. 1547\)](#). For more information about upgrade considerations, see [Time zone considerations \(p. 1762\)](#).

Considerations for setting the time zone

The time zone option is a permanent and persistent option. Therefore, you can't do the following:

- Remove the option from an option group after you add the option.
- Remove the option group from a DB instance after you add the group.
- Modify the time zone setting of the option to a different time zone.

If you accidentally set the time zone incorrectly, you need to recover the DB instance to its previous time zone setting. We strongly urge you to use one of the following strategies, depending on your situation:

- Your DB instance currently uses the default option group.

Take a snapshot of your DB instance, and then add the time zone option to your DB instance. For more information, see [Creating a DB snapshot \(p. 448\)](#).

- Your DB instance currently uses a nondefault option group.

Take a snapshot of your DB instance, create a new option group with the time zone option, and then add the option group to your instance.

We strongly urge you to test the time zone option on a test DB instance before you add it to a production DB instance. Adding the time zone option can cause problems with tables that use system date to add dates or times. We recommend that you analyze your data and applications to determine the impact of changing the time zone.

Time zone option settings

Amazon RDS supports the following settings for the time zone option.

Option setting	Valid values	Description
TIME_ZONE	One of the available time zones. For the full list, see Available time zones (p. 1744) .	The new time zone for your DB instance.

Adding the time zone option

The general process for adding the time zone option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.

2. Add the option to the option group.
3. Associate the option group with the DB instance.

When you add the time zone option, a brief outage occurs while your DB instance is automatically restarted.

Console

To add the time zone option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine** choose the oracle edition for your DB instance.
 - b. For **Major engine version** choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **Timezone** option to the option group, and configure the option settings.

Important

If you add the time zone option to an existing option group that is already attached to one or more DB instances, a brief outage occurs while all the DB instances are automatically restarted.

For more information about adding options, see [Adding an option to an option group \(p. 277\)](#). For more information about each setting, see [Time zone option settings \(p. 1742\)](#).

3. Apply the option group to a new or existing DB instance:

- For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. When you add the time zone option to an existing DB instance, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

The following example uses the AWS CLI `add-option-to-option-group` command to add the `Timezone` option and the `TIME_ZONE` option setting to an option group called `myoptiongroup`. The time zone is set to Africa/Cairo.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
--option-group-name "myoptiongroup" \
--options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/Cairo}]" \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name "myoptiongroup" ^
--options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/Cairo}]" ^
--apply-immediately
```

Modifying time zone settings

The time zone option is a permanent and persistent option. You can't remove the option from an option group after you add it. You can't remove the option group from a DB instance after you add it. You can't modify the time zone setting of the option to a different time zone. If you set the time zone incorrectly, restore a snapshot of your DB instance from before you added the time zone option.

Removing the time zone option

The time zone option is a permanent and persistent option. You can't remove the option from an option group after you add it. You can't remove the option group from a DB instance after you add it. To remove the time zone option, restore a snapshot of your DB instance from before you added the time zone option.

Available time zones

You can use the following values for the time zone option.

Zone	Time zone
Africa	Africa/Cairo, Africa/Casablanca, Africa/Harare, Africa/Lagos, Africa/Luanda, Africa/Monrovia, Africa/Nairobi, Africa/Tripoli, Africa/Windhoek
America	America/Araguaina, America/Argentina/Buenos_Aires, America/Asuncion, America/Bogota, America/Caracas, America/Chicago, America/Chihuahua, America/Cuiaba, America/Denver, America/Detroit, America/Fortaleza, America/Godthab, America/Guatemala, America/Halifax, America/Lima, America/Los_Angeles, America/Manaus, America/Matamoros, America/Mexico_City, America/Monterrey, America/Montevideo, America/New_York, America/Phoenix, America/Santiago, America/Sao_Paulo, America/Tijuana, America/Toronto
Asia	Asia/Amman, Asia/Ashgabat, Asia/Baghdad, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Calcutta, Asia/Damascus, Asia/Dhaka, Asia/Hong_Kong, Asia/Irkutsk, Asia/Jakarta, Asia/Jerusalem, Asia/Kabul, Asia/Karachi, Asia/Kathmandu, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Magadan, Asia/Manila, Asia/Muscat, Asia/Novosibirsk, Asia/Rangoon, Asia/Riyadh, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tehran, Asia/Tokyo, Asia/Ulaanbaatar, Asia/Vladivostok, Asia/Yakutsk, Asia/Yerevan
Atlantic	Atlantic/Azores, Atlantic/Cape_Verde
Australia	Australia/Adelaide, Australia/Brisbane, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/Lord_Howe, Australia/Perth, Australia/Sydney
Brazil	Brazil/DeNoronha, Brazil/East
Canada	Canada/Newfoundland, Canada/Saskatchewan
Etc	Etc/GMT-3
Europe	Europe/Amsterdam, Europe/Athens, Europe/Berlin, Europe/Dublin, Europe/Helsinki, Europe/Kaliningrad, Europe/London, Europe/Madrid, Europe/Moscow, Europe/Paris, Europe/Prague, Europe/Rome, Europe/Sarajevo
Pacific	Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Fiji, Pacific/Guam, Pacific/Honolulu, Pacific/Kiritimati, Pacific/Marquesas, Pacific/Samoa, Pacific/Tongatapu, Pacific/Wake

Zone	Time zone
US	US/Alaska, US/Central, US/East-Indiana, US/Eastern, US/Pacific
UTC	UTC

Oracle time zone file autoupgrade

With the TIMEZONE_FILE_AUTOUPGRADE option, you can upgrade the current time zone file to the latest version on your DB instance.

Topics

- [Purpose of time zone files \(p. 1746\)](#)
- [Considerations for updating your time zone file \(p. 1746\)](#)
- [Strategies for updating your time zone file \(p. 1747\)](#)
- [Preparing to update the time zone file \(p. 1748\)](#)
- [Adding the time zone file autoupgrade option \(p. 1749\)](#)
- [Checking your data after the update of the time zone file \(p. 1750\)](#)

Purpose of time zone files

In Oracle Database, the TIMESTAMP WITH TIME ZONE data type stores time stamp and time zone data. This data type is useful for preserving local time zone information.

Oracle Database stores transition rules and UTC offsets in *time zone files*. The offset is the difference between local time and UTC. When you create an Oracle database in an on-premises environment, you choose the time zone file version. Data with the TIMESTAMP WITH TIME ZONE data type uses the rules in the associated time zone file version. The time zone files reside in \$ORACLE_HOME/oracore/zoneinfo/.

If a government changes the rules for Daylight Savings Time (DST), Oracle publishes new time zone files. Oracle releases time zone files separately from PSUs and RUs. The time zone file names use the format DSTv`version`, as in DSTv35. When you add the TIMEZONE_FILE_AUTOUPGRADE option in Amazon RDS for Oracle, you can update your time zone files.

The TIMEZONE_FILE_AUTOUPGRADE option is useful when you move data between different environments. If you try to import data from a source database with a higher time zone file version than the target database, you receive the ORA-39405 error. Previously, you had to work around the error by using either of the following techniques:

- Create an RDS for Oracle instance with the desired time zone file, export data from your source database, and then import it into the new database.
- Use AWS DMS or logical replication to migrate your data.

With the TIMEZONE_FILE_AUTOUPGRADE option, you can upgrade the time zone file on the source database without using the preceding cumbersome techniques.

Considerations for updating your time zone file

When you update your time zone file, data that uses TIMESTAMP WITH TIME ZONE might change. Your primary consideration is downtime.

Warning

If you add the TIMEZONE_FILE_AUTOUPGRADE, your engine upgrade might have prolonged downtime. Updating time zone data for a large database might take hours or even days.

The length of the update depends on factors such as the following:

- The amount of TIMESTAMP WITH TIME ZONE data in your database

- The instance configuration
- The DB instance class
- The storage configuration
- The database configuration
- The database parameter settings

Additional downtime can occur when you do the following:

- Add the option to the option group when the instance uses an outdated time zone file
- Upgrade the Oracle database engine when the new engine version contains a new version of the time zone file

Note

During the time zone file update, RDS for Oracle calls PURGE DBA_RECYCLEBIN.

Strategies for updating your time zone file

You can upgrade your engine and update your time zone file independently. Thus, you must choose among different update strategies.

The examples in this section assume that your instance uses database version 19.0.0.0.ru-2019-07.rur-2019-07.r1 and time zone file DSTv33. Your DB instance file system includes file DSTv34. Also assume that release update 19.0.0.0.ru-2021-01.rur-2021-01.r1 includes DSTv35. To update your time zone file, you can use the following strategies:

- Update the time zone file used by your database without upgrading the DB engine version.

Update the time zone file used by your instance from DSTv33 to DSTv34. In your modify instance operation, do the following:

- Add TIMEZONE_FILE_AUTOUPGRADE to the option group used by your instance.
- Don't change your engine version.
- Upgrade your DB engine version and the time zone file in the same operation.

Upgrade your engine to version 19.0.0.0.ru-2021-01.rur-2021-01.r1 and update your time zone file to DSTv35 in the same operation. In your modify instance operation, do the following:

- Add TIMEZONE_FILE_AUTOUPGRADE to the option group used by your instance.
- Change your engine version.
- Upgrade your DB engine version without updating the time zone file.

Upgrade your database to version 19.0.0.0.ru-2021-01.rur-2021-01.r1 but retain time zone file DSTv33. In this case, the possibilities are as follows:

- Your instance isn't associated with an option group that includes TIMEZONE_FILE_AUTOUPGRADE. Leave the option group as it is.
- Your instance is associated with an option group that includes TIMEZONE_FILE_AUTOUPGRADE. Associate your instance with an option group that doesn't have TIMEZONE_FILE_AUTOUPGRADE. Then modify the engine version.

You might choose this strategy for the following reasons:

- Your data doesn't use the TIMESTAMP WITH TIME ZONE data type.
- Your data uses the TIMESTAMP WITH TIME ZONE data type, but your data is not affected by the time zone changes.
- You want to postpone updating the time zone file because you can't tolerate the extra downtime.

Preparing to update the time zone file

A time zone file upgrade has two separate phases: prepare and upgrade. While not required, we strongly recommend that you perform the prepare step. In this step, you find out which data will be affected by running the PL/SQL procedure DBMS_DST.FIND_AFFECTED_TABLES. For more information about the prepare window, see [Upgrading the Time Zone File and Timestamp with Time Zone Data](#) in the Oracle Database documentation.

To prepare to update the time zone file

1. Connect to your Oracle database using a SQL client.
2. Determine the current timezone file version used.

```
SELECT * FROM V$TIMEZONE_FILE;
```

3. Determine the latest timezone file version available on your DB instance. This step is only applicable if you use Oracle Database 12c Release 2 (12.2) or higher.

```
SELECT DBMS_DST.GET_LATEST_TIMEZONE_VERSION FROM DUAL;
```

4. Determine the total size of tables that have columns of type TIMESTAMP WITH LOCAL TIME ZONE or TIMESTAMP WITH TIME ZONE.

```
SELECT SUM(BYTES)/1024/1024/1024 "Total_size_w_TSTZ_columns_GB"  
FROM   DBA_SEGMENTS  
WHERE  SEGMENT_TYPE LIKE 'TABLE%'  
AND    (OWNER, SEGMENT_NAME) IN  
       (SELECT OWNER, TABLE_NAME  
        FROM   DBA_TAB_COLUMNS  
        WHERE  DATA_TYPE LIKE 'TIMESTAMP%TIME ZONE');
```

5. Determine the names and sizes of segments that have columns of type TIMESTAMP WITH LOCAL TIME ZONE or TIMESTAMP WITH TIME ZONE.

```
SELECT OWNER, SEGMENT_NAME, SUM(BYTES)/1024/1024/1024 "SEGMENT_SIZE_W_TSTZ_COLUMNS_GB"  
FROM   DBA_SEGMENTS  
WHERE  SEGMENT_TYPE LIKE 'TABLE%'  
AND    (OWNER, SEGMENT_NAME) IN  
       (SELECT OWNER, TABLE_NAME  
        FROM   DBA_TAB_COLUMNS  
        WHERE  DATA_TYPE LIKE 'TIMESTAMP%TIME ZONE')  
GROUP BY OWNER, SEGMENT_NAME;
```

6. Run the prepare step.

- The procedure DBMS_DST.CREATE_AFFECTED_TABLE creates a table to store any affected data. You pass the name of this table to the DBMS_DST.FIND_AFFECTED_TABLES procedure. For more information, see [CREATE_AFFECTED_TABLE Procedure](#) in the Oracle Database documentation.
- This procedure CREATE_ERROR_TABLE creates a table to log errors. For more information, see [CREATE_ERROR_TABLE Procedure](#) in the Oracle Database documentation.

The following example creates the affected data and error tables, and finds all affected tables.

```
EXEC DBMS_DST.CREATE_ERROR_TABLE('my_error_table')  
EXEC DBMS_DST.CREATE_AFFECTED_TABLE('my_affected_table')  
  
EXEC DBMS_DST.BEGIN_PREPARE(new_version);  
EXEC DBMS_DST.FIND_AFFECTED_TABLES('my_affected_table', TRUE, 'my_error_table');
```

```
EXEC DBMS_DST.END_PREPARE;  
  
SELECT * FROM my_affected_table;  
SELECT * FROM my_error_table;
```

7. Query the affected and error tables.

```
SELECT * FROM my_affected_table;  
SELECT * FROM my_error_table;
```

Adding the time zone file autoupgrade option

The procedure for adding the time zone autoupgrade option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.
3. Associate the option group with the DB instance.

When you add the option, a brief outage occurs while your DB instance is automatically restarted.

Console

To add the time zone file autoupgrade option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:
 - a. For **Engine** choose the oracle edition for your DB instance.
 - b. For **Major engine version** choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **TIMEZONE_FILE_AUTOUPGRADE** option to the option group.

Important

If you add the option to an existing option group that is already attached to one or more DB instances, a brief outage occurs while all the DB instances are automatically restarted.

3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. When you add the time zone option to an existing DB instance, a brief outage occurs while your DB instance is automatically restarted. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

AWS CLI

The following example uses the AWS CLI **add-option-to-option-group** command to add the **TIMEZONE_FILE_AUTOUPGRADE** option to an option group called **myoptiongroup**.

For Linux, macOS, or Unix:

```
aws rds add-option-to-option-group \
```

```
--option-group-name "myoptiongroup" \
--options "OptionName=TIMEZONE_FILE_AUTOUPGRADE" \
--apply-immediately
```

For Windows:

```
aws rds add-option-to-option-group ^
--option-group-name "myoptiongroup" ^
--options "OptionName=TIMEZONE_FILE_AUTOUPGRADE" ^
--apply-immediately
```

Checking your data after the update of the time zone file

We recommend that you check your data after you update the time zone file. During the prepare step, RDS for Oracle automatically creates the following tables:

- `rdsadmin.rds_dst_affected_tables` – Lists the tables that contain data affected by the update
- `rdsadmin.rds_dst_error_table` – Lists the errors generated during the update

These tables are independent of any tables that you create in the prepare window. To see the results of the update, query the tables as follows.

```
SELECT * FROM rdsadmin.rds_dst_affected_tables;
SELECT * FROM rdsadmin.rds_dst_error_table;
```

For more information about the schema for the affected data and error tables, see [FIND_AFFECTED_TABLES Procedure](#) in the Oracle documentation.

Oracle Transparent Data Encryption

Amazon RDS supports Oracle Transparent Data Encryption (TDE), a feature of the Oracle Advanced Security option available in Oracle Enterprise Edition. This feature automatically encrypts data before it is written to storage and automatically decrypts data when the data is read from storage.

Oracle Transparent Data Encryption is used in scenarios where you need to encrypt sensitive data in case data files and backups are obtained by a third party or when you need to address security-related regulatory compliance issues.

The TDE option is a permanent option that can't be removed from an option group. You can't disable TDE from a DB instance once that instance is associated with an option group with the Oracle TDE option. You can change the option group of a DB instance that is using the TDE option, but the option group associated with the DB instance must include the TDE option. You can also modify an option group that includes the TDE option by adding or removing other options.

A detailed explanation about Oracle Transparent Data Encryption is beyond the scope of this guide. For information about using Oracle Transparent Data Encryption, see [Securing stored data using Transparent Data Encryption](#). For more information about Oracle Advanced Security, see [Oracle advanced security](#) in the Oracle documentation. For more information on AWS security, see the [AWS security center](#).

Note

You can't share a DB snapshot that uses this option. For more information about sharing DB snapshots, see [Sharing a DB snapshot \(p. 472\)](#).

TDE encryption modes

Oracle Transparent Data Encryption supports two encryption modes: TDE tablespace encryption and TDE column encryption. TDE tablespace encryption is used to encrypt entire application tables. TDE column encryption is used to encrypt individual data elements that contain sensitive data. You can also apply a hybrid encryption solution that uses both TDE tablespace and column encryption.

Note

Amazon RDS manages the Oracle Wallet and TDE master key for the DB instance. You do not need to set the encryption key using the command ALTER SYSTEM set encryption key.

For information about TDE best practices, see [Oracle advanced security Transparent Data Encryption best practices](#).

Once the option is enabled, you can check the status of the Oracle Wallet by using the following command:

```
SELECT * FROM v$encryption_wallet;
```

To create an encrypted tablespace, use the following command:

```
CREATE TABLESPACE encrypt_ts ENCRYPTION DEFAULT STORAGE (ENCRYPT);
```

To specify the encryption algorithm, use the following command:

```
CREATE TABLESPACE encrypt_ts ENCRYPTION USING 'AES256' DEFAULT STORAGE (ENCRYPT);
```

Note that the previous commands for encrypting a tablespace are the same as the commands you would use with an Oracle installation not on Amazon RDS, and the ALTER TABLE syntax to encrypt a column is also the same as the commands you would use for an Oracle installation not on Amazon RDS.

You should determine if your DB instance is associated with an option group that has the **TDE** option. To view the option group that a DB instance is associated with, you can use the RDS console, the [describe-db-instance](#) AWS CLI command, or the API operation [DescribeDBInstances](#).

To comply with several security standards, Amazon RDS is working to implement automatic periodic master key rotation.

Adding the TDE option

The process for using Oracle Transparent Data Encryption (TDE) with Amazon RDS is as follows:

1. If the DB instance is not associated with an option group that has the **TDE** option enabled, you must either create an option group and add the **TDE** option or modify the associated option group to add the **TDE** option. For information about creating or modifying an option group, see [Working with option groups \(p. 273\)](#). For information about adding an option to an option group, see [Adding an option to an option group \(p. 277\)](#).
2. Associate the DB instance with the option group with the **TDE** option. For information about associating a DB instance with an option group, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Removing the TDE option

To remove the **TDE** option with a DB instance, complete the following steps:

1. Decrypt all your data on the DB instance.
2. Copy the data to a new DB instance that is not associated with an option group with **TDE** enabled.
3. Delete the original instance.

You can name the new instance the same name as the previous DB instance.

Using TDE with Oracle Data Pump

You can use Oracle Data Pump to import or export encrypted dump files. Amazon RDS supports the password encryption mode (ENCRYPTION_MODE=PASSWORD) for Oracle Data Pump. Amazon RDS does not support transparent encryption mode (ENCRYPTION_MODE=TRANSPARENT) for Oracle Data Pump. For more information about using Oracle Data Pump with Amazon RDS, see [Importing using Oracle Data Pump \(p. 1616\)](#).

Oracle UTL_MAIL

Amazon RDS supports Oracle UTL_MAIL through the use of the UTL_MAIL option and SMTP servers. You can send email directly from your database by using the UTL_MAIL package. Amazon RDS supports UTL_MAIL for the following versions of Oracle:

- Oracle Database 21c (21.0.0.0), all versions
- Oracle Database 19c (19.0.0.0), all versions
- Oracle Database 12c Release 2 (12.2), all versions
- Oracle Database 12c Release 1 (12.1), version 12.1.0.2.v5 and later

The following are some limitations to using UTL_MAIL:

- UTL_MAIL does not support Transport Layer Security (TLS) and therefore emails are not encrypted.

To connect securely to remote SSL/TLS resources by creating and uploading custom Oracle wallets, follow the instructions in [Configuring UTL_HTTP access using certificates and an Oracle wallet \(p. 1513\)](#).

The specific certificates that are required for your wallet vary by service. For AWS services, these can typically be found in the [Amazon trust services repository](#).

- UTL_MAIL does not support authentication with SMTP servers.
- You can only send a single attachment in an email.
- You can't send attachments larger than 32 K.
- You can only use ASCII and Extended Binary Coded Decimal Interchange Code (EBCDIC) character encodings.
- SMTP port (25) is throttled based on the elastic network interface owner's policies.

When you enable UTL_MAIL, only the master user for your DB instance is granted the execute privilege. If necessary, the master user can grant the execute privilege to other users so that they can use UTL_MAIL.

Important

We recommend that you enable Oracle's built-in auditing feature to track the use of UTL_MAIL procedures.

Prerequisites for Oracle UTL_MAIL

The following are prerequisites for using Oracle UTL_MAIL:

- One or more SMTP servers, and the corresponding IP addresses or public or private Domain Name Server (DNS) names. For more information about private DNS names resolved through a custom DNS server, see [Setting up a custom DNS server \(p. 1539\)](#).
- For Oracle versions prior to 12c, your DB instance must also use the XML DB option. For more information, see [Oracle XML DB \(p. 1756\)](#).

Adding the Oracle UTL_MAIL option

The general process for adding the Oracle UTL_MAIL option to a DB instance is the following:

1. Create a new option group, or copy or modify an existing option group.
2. Add the option to the option group.

3. Associate the option group with the DB instance.

After you add the UTL_MAIL option, as soon as the option group is active, UTL_MAIL is active.

To add the UTL_MAIL option to a DB instance

1. Determine the option group you want to use. You can create a new option group or use an existing option group. If you want to use an existing option group, skip to the next step. Otherwise, create a custom DB option group with the following settings:

- a. For **Engine**, choose the edition of Oracle you want to use.
- b. For **Major engine version**, choose the version of your DB instance.

For more information, see [Creating an option group \(p. 274\)](#).

2. Add the **UTL_MAIL** option to the option group. For more information about adding options, see [Adding an option to an option group \(p. 277\)](#).
3. Apply the option group to a new or existing DB instance:
 - For a new DB instance, you apply the option group when you launch the instance. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
 - For an existing DB instance, you apply the option group by modifying the instance and attaching the new option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Using Oracle UTL_MAIL

After you enable the UTL_MAIL option, you must configure the SMTP server before you can begin using it.

You configure the SMTP server by setting the **SMTP_OUT_SERVER** parameter to a valid IP address or public DNS name. For the **SMTP_OUT_SERVER** parameter, you can specify a comma-separated list of the addresses of multiple servers. If the first server is unavailable, UTL_MAIL tries the next server, and so on.

You can set the default **SMTP_OUT_SERVER** for a DB instance by using a [DB parameter group](#). You can set the **SMTP_OUT_SERVER** parameter for a session by running the following code on your database on your DB instance.

```
ALTER SESSION SET smtp_out_server = mailserver.domain.com:25;
```

After the UTL_MAIL option is enabled, and your **SMTP_OUT_SERVER** is configured, you can send mail by using the **SEND** procedure. For more information, see [UTL_MAIL](#) in the Oracle documentation.

Removing the Oracle UTL_MAIL option

You can remove Oracle UTL_MAIL from a DB instance.

To remove UTL_MAIL from a DB instance, do one of the following:

- To remove UTL_MAIL from multiple DB instances, remove the UTL_MAIL option from the option group they belong to. This change affects all DB instances that use the option group. For more information, see [Removing an option from an option group \(p. 285\)](#).
- To remove UTL_MAIL from a single DB instance, modify the DB instance and specify a different option group that doesn't include the UTL_MAIL option. You can specify the default (empty) option

group, or a different custom option group. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Troubleshooting

The following are issues you might encounter when you use UTL_MAIL with Amazon RDS.

- **Throttling.** SMTP port (25) is throttled based on the elastic network interface owner's policies. If you can successfully send email by using UTL_MAIL, and you see the error ORA-29278: SMTP transient error: 421 Service not available, you are possibly being throttled. If you experience throttling with email delivery, we recommend that you implement a backoff algorithm. For more information about backoff algorithms, see [Error retries and exponential backoff in AWS](#) and [How to handle a "throttling – Maximum sending rate exceeded" error](#).

You can request that this throttle be removed. For more information, see [How do I remove the throttle on port 25 from my EC2 instance?](#).

Oracle XML DB

Oracle XML DB adds native XML support to your DB instance. With XML DB, you can store and retrieve structured or unstructured XML, in addition to relational data. XML DB is preinstalled on Oracle version 12c and later.

Upgrading the RDS for Oracle DB engine

When Amazon RDS supports a new version of Oracle, you can upgrade your DB instances to the new version. For information about which Oracle versions are available on Amazon RDS, see [Amazon RDS for Oracle Release Notes](#).

Important

RDS for Oracle Database 11g is deprecated. If you maintain Oracle Database 11g snapshots, you can upgrade them to a later release. For more information, see [Upgrading an Oracle DB snapshot \(p. 1764\)](#).

Topics

- [Overview of RDS for Oracle engine upgrades \(p. 1757\)](#)
- [Oracle major version upgrades \(p. 1759\)](#)
- [Oracle minor version upgrades \(p. 1760\)](#)
- [Considerations for Oracle DB upgrades \(p. 1761\)](#)
- [Testing an Oracle DB upgrade \(p. 1763\)](#)
- [Upgrading an Oracle DB instance \(p. 1764\)](#)
- [Upgrading an Oracle DB snapshot \(p. 1764\)](#)

Overview of RDS for Oracle engine upgrades

Before upgrading your RDS for Oracle DB instance, familiarize yourself with the following concepts.

Topics

- [Major and minor version upgrades \(p. 1757\)](#)
- [Expected support dates for RDS for Oracle major releases \(p. 1758\)](#)
- [Oracle engine version management \(p. 1758\)](#)
- [Automatic snapshots during engine upgrades \(p. 1758\)](#)
- [Oracle upgrades in a Multi-AZ deployment \(p. 1759\)](#)
- [Oracle upgrades of read replicas \(p. 1759\)](#)
- [Oracle upgrades of micro DB instances \(p. 1759\)](#)

Major and minor version upgrades

Amazon RDS supports the following upgrades to an Oracle DB instance:

- Major version upgrades

In general, a *major version upgrade* for a database engine can introduce changes that aren't compatible with existing applications. To upgrade your DB instance to a major version, you must perform the action manually.

- Minor version upgrades

A *minor version upgrade* includes only changes that are backward-compatible with existing applications. If you enable auto minor version upgrades on your DB instance, minor version upgrades occur automatically. In all other cases, you upgrade the DB instance manually.

When you upgrade the DB engine, an outage occurs. The duration of the outage depends on your engine version and instance size.

Expected support dates for RDS for Oracle major releases

RDS for Oracle major versions remain available at least until the end of support date for the corresponding Oracle Database release version. You can use the following dates to plan your testing and upgrade cycles. These dates represent the earliest date that an upgrade to a newer version might be required. If Amazon extends support for an RDS for Oracle version for longer than originally stated, we plan to update this table to reflect the later date.

Oracle Database major release version	Expected date for upgrading to a newer version
Oracle Database 19c	April 30, 2024 without Extended Support or an Unlimited License Agreement
	April 30, 2027 with Extended Support or an Unlimited License Agreement
Oracle Database 21c	April 30, 2024

Before we ask that you upgrade to a newer major version and to help you plan, we provide a reminder at least 12 months in advance. We do so to communicate the detailed upgrade process. Details include the timing of certain milestones, the impact on your DB instances, and the actions that we recommend that you take. We recommend that you thoroughly test your applications with new RDS for Oracle versions before performing a major version upgrade.

After this advance notification period, an automatic upgrade to the subsequent major version might be applied to any RDS for Oracle DB instance still running the older version. If so, the upgrade is started during scheduled maintenance windows.

Oracle engine version management

With DB engine version management, you control when and how the database engine is patched and upgraded. You get the flexibility to maintain compatibility with database engine patch versions. You can also test new patch versions of RDS for Oracle to ensure they work with your application before deploying them in production. In addition, you upgrade the versions on your own terms and timelines.

Note

Amazon RDS periodically aggregates official Oracle database patches using an Amazon RDS-specific DB engine version. To see a list of which Oracle patches are contained in an Amazon RDS Oracle-specific engine version, go to [Amazon RDS for Oracle Release Notes](#).

Automatic snapshots during engine upgrades

During upgrades of an Oracle DB instance, snapshots offer protection against upgrade issues. If the backup retention period for your DB instance is greater than 0, Amazon RDS takes the following DB snapshots during the upgrade:

1. A snapshot of the DB instance before any upgrade changes have been made. If the upgrade fails, you can restore this snapshot to create a DB instance running the old version.
2. A snapshot of the DB instance after the upgrade completes.

Note

To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

After an upgrade, you can't revert to the previous engine version. However, you can create a new Oracle DB instance by restoring the pre-upgrade snapshot.

Oracle upgrades in a Multi-AZ deployment

If your DB instance is in a Multi-AZ deployment, Amazon RDS upgrades both the primary and standby replicas. If no operating system updates are required, the primary and standby upgrades occur simultaneously. The instances are not available until the upgrade completes.

If operating system updates are required in a Multi-AZ deployment, Amazon RDS applies the updates when you request the DB upgrade. Amazon RDS performs the following steps:

1. Updates the operating system on the standby DB instance.
2. Upgrades the standby DB instance.
3. Fails over the primary instance to the standby DB instance.
4. Upgrades the operating system on the new standby DB instance, which was formerly the primary instance.
5. Upgrades the new standby DB instance.

Oracle upgrades of read replicas

The Oracle DB engine version of the source DB instance and all of its read replicas must be the same. Amazon RDS performs the upgrade in the following stages:

1. Upgrades the source DB instance. The read replicas are available during this stage.
2. Upgrades the read replicas in parallel, regardless of the replica maintenance windows. The source DB is available during this stage.

For major version upgrades of cross-Region read replicas, Amazon RDS performs additional actions:

- Generates an option group for the target version automatically
- Copies all options and option settings from the original option group to the new option group
- Associates the upgraded cross-Region read replica with the new option group

Oracle upgrades of micro DB instances

We don't recommend upgrading databases running on micro DB instances. Because these instances have limited CPU, the upgrade can take hours to complete.

You can upgrade micro DB instances with small amounts of storage (10–20 GiB) by copying your data using Data Pump. Before you migrate your production DB instances, we recommend that you test by copying data using Data Pump.

Oracle major version upgrades

To perform a major version upgrade, modify the DB instance manually. Major version upgrades don't occur automatically.

Supported versions for major upgrades

Amazon RDS supports the following major version upgrades.

Current version	Upgrade supported
19.0.0.0 using the CDB architecture	21.0.0.0

A major version upgrade of Oracle Database must upgrade to a Release Update (RU) that was released in the same month or later. Major version downgrades aren't supported for any Oracle Database versions.

Supported instance classes for major upgrades

Your current Oracle DB instance might run on a DB instance class that isn't supported for the version to which you are upgrading. In this case, before you upgrade, migrate the DB instance to a supported DB instance class. For more information about the supported DB instance classes for each version and edition of Amazon RDS for Oracle, see [DB instance classes \(p. 10\)](#).

Gathering statistics before major upgrades

Before you perform a major version upgrade, Oracle recommends that you gather optimizer statistics on the DB instance that you are upgrading. This action can reduce DB instance downtime during the upgrade.

To gather optimizer statistics, connect to the DB instance as the master user, and run the DBMS_STATS.GATHER_DICTIONARY_STATS procedure, as in the following example.

```
EXEC DBMS_STATS.GATHER_DICTIONARY_STATS;
```

For more information, see [Gathering optimizer statistics to decrease Oracle database downtime](#) in the Oracle documentation.

Allowing major upgrades

A major engine version upgrade might be incompatible with your application. The upgrade is irreversible. If you specify a major version for the EngineVersion parameter that is different from the current major version, you must allow major version upgrades.

If you upgrade a major version using the CLI command [modify-db-instance](#), specify --allow-major-version-upgrade. This setting isn't persistent, so you must specify --allow-major-version-upgrade whenever you perform a major upgrade. This parameter has no impact on upgrades of minor engine versions. For more information, see [Upgrading a DB instance engine version \(p. 360\)](#).

If you upgrade a major version using the console, you don't need to choose an option to allow the upgrade. Instead, the console displays a warning that major upgrades are irreversible.

Oracle minor version upgrades

A minor version upgrade applies an Oracle Database Patch Set Update (PSU) or Release Update (RU) in a major version.

An Amazon RDS for Oracle DB instance is scheduled to be upgraded automatically during its next maintenance window when it meets the following conditions:

- The DB instance has the **Auto minor version upgrade** option enabled.
- The DB instance is not running the latest minor DB engine version.

Amazon RDS for Oracle upgrades your DB instance to the latest quarterly RU or RUR four to six weeks after it is made available. For more information about RUs and RURs, see [Amazon RDS for Oracle Release Notes](#).

Note

RDS for Oracle doesn't support minor version downgrades.

Considerations for Oracle DB upgrades

Before you upgrade your Oracle instance, review the following information.

Topics

- [Oracle Multitenant considerations \(p. 1761\)](#)
- [Option group considerations \(p. 1761\)](#)
- [Parameter group considerations \(p. 1762\)](#)
- [Time zone considerations \(p. 1762\)](#)
- [Oracle Database 12c upgrade considerations \(p. 1762\)](#)

Oracle Multitenant considerations

The following table describes the architectures supported in different releases.

Oracle Database release	Architecture
Oracle Database 21c	CDB only
Oracle Database 19c	CDB or non-CDB
Oracle Database 12c Release 2 (12.2)	Non-CDB only
Oracle Database 12c Release 1 (12.1)	Non-CDB only

The following table describes supported and unsupported upgrade paths.

Upgrade path	Supported?
Non-CDB to non-CDB	Yes
CDB to CDB	Yes
Non-CDB to CDB	No
CDB to non-CDB	No

For more information about Oracle Multitenant in RDS for Oracle, see [RDS for Oracle architecture \(p. 1480\)](#).

Option group considerations

If your DB instance uses a custom option group, sometimes Amazon RDS can't automatically assign a new option group. For example, this situation occurs when you upgrade to a new major version. In such cases, specify a new option group when you upgrade. We recommend that you create a new option group, and add the same options to it as in your existing custom option group.

For more information, see [Creating an option group \(p. 274\)](#) or [Copying an option group \(p. 276\)](#).

If your DB instance uses a custom option group that contains the APEX option, you can sometimes reduce the upgrade time. To do this, upgrade your version of APEX at the same time as your DB instance. For more information, see [Upgrading the APEX version \(p. 1673\)](#).

Parameter group considerations

If your DB instance uses a custom parameter group, sometimes Amazon RDS can't automatically assign your DB instance a new parameter group. For example, this situation occurs when you upgrade to a new major version. In such cases, make sure to specify a new parameter group when you upgrade. We recommend that you create a new parameter group, and configure the parameters as in your existing custom parameter group.

For more information, see [Creating a DB parameter group \(p. 291\)](#) or [Copying a DB parameter group \(p. 298\)](#).

Time zone considerations

You can use the time zone option to change the *system time zone* used by your Oracle DB instance. For example, you might change the time zone of a DB instance to be compatible with an on-premises environment, or a legacy application. The time zone option changes the time zone at the host level. Amazon RDS for Oracle updates the system time zone automatically throughout the year. For more information about the system time zone, see [Oracle time zone \(p. 1742\)](#).

When you create an Oracle DB instance, the database automatically sets the *database time zone*. The database time zone is also known as the Daylight Saving Time (DST) time zone. The database time zone is distinct from the system time zone.

Between Oracle Database releases, patch sets or individual patches may include new DST versions. These patches reflect the changes in transition rules for various time zone regions. For example, a government might change when DST takes effect. Changes to DST rules may affect existing data of the `TIMESTAMP WITH TIME ZONE` data type.

If you upgrade an RDS for Oracle DB instance, Amazon RDS doesn't upgrade the database time zone file automatically. To upgrade the time zone file automatically, you can include the `TIMEZONE_FILE_AUTOUPGRADE` option in the option group associated with your DB instance during or after the engine version upgrade. For more information, see [Oracle time zone file autoupgrade \(p. 1746\)](#).

Alternatively, to upgrade the database time zone file manually, create a new Oracle DB instance that has the desired DST patch. However, we recommend that you upgrade the database time zone file using the `TIMEZONE_FILE_AUTOUPGRADE` option.

After upgrading the time zone file, migrate the data from your current instance to the new instance. You can migrate data using several techniques, including the following:

- AWS Database Migration Service
- Oracle GoldenGate
- Oracle Data Pump
- Original Export/Import (desupported for general use)

Note

When you migrate data using Oracle Data Pump, the utility raises the error ORA-39405 when the target time zone version is lower than the source time zone version.

For more information, see [TIMESTAMP WITH TIMEZONE restrictions](#) in the Oracle documentation.

Oracle Database 12c upgrade considerations

Amazon RDS has deprecated support for Oracle Database 12c on both Oracle Enterprise Edition and Oracle Standard Edition 2. As explained in [Oracle Database 12c with Amazon RDS \(p. 1473\)](#), Amazon RDS

began automatically upgrading Oracle Database 12c DB instances to Oracle Database 19c. You can no longer upgrade manually. The automatic upgrades began on the following dates:

- April 1, 2022 for Oracle Database 12c Release 2 (12.2.0.1)
- August 1, 2022 for Oracle Database 12c Release 1 (12.1.0.2)

The automatic upgrades are not guaranteed to occur in your maintenance window. All Oracle Database 12c DB instances, including reserved instances, will move to the latest available Release Update (RU).

After your Oracle Database 12c DB instance is upgraded to Oracle Database 19c, consider the following:

- Your SQL statements might perform differently after the upgrade. If so, you can use the OPTIMIZER_FEATURES_ENABLE parameter to retain the behavior of the Oracle Database 12c optimizer. For more information, see [Influencing the Optimizer](#) in the Oracle Database documentation.
- If you have Extended Support for Oracle Database 12c on the BYOL model, consider the implications. In this case, you must have Extended Support agreements from Oracle Support for Oracle Database 19c. For details on licensing and support requirements for BYOL, see [Amazon RDS for Oracle FAQs](#).

Testing an Oracle DB upgrade

Before you upgrade your DB instance to a major version, thoroughly test your database and all applications that access the database for compatibility with the new version. We recommend that you use the following procedure.

To test a major version upgrade

1. Review the Oracle upgrade documentation for the new version of the database engine to see if there are compatibility issues that might affect your database or applications. For more information, see [Database Upgrade Guide](#) in the Oracle documentation.
2. If your DB instance uses a custom option group, create a new option group compatible with the new version you are upgrading to. For more information, see [Option group considerations \(p. 1761\)](#).
3. If your DB instance uses a custom parameter group, create a new parameter group compatible with the new version you are upgrading to. For more information, see [Parameter group considerations \(p. 1762\)](#).
4. Create a DB snapshot of the DB instance to be upgraded. For more information, see [Creating a DB snapshot \(p. 448\)](#).
5. Restore the DB snapshot to create a new test DB instance. For more information, see [Restoring from a DB snapshot \(p. 452\)](#).
6. Modify this new test DB instance to upgrade it to the new version, by using one of the following methods:
 - [Console \(p. 360\)](#)
 - [AWS CLI \(p. 361\)](#)
 - [RDS API \(p. 361\)](#)
7. Perform testing:
 - Run as many of your quality assurance tests against the upgraded DB instance as needed to ensure that your database and application work correctly with the new version.
 - Implement any new tests needed to evaluate the impact of any compatibility issues that you identified in step 1.
 - Test all stored procedures, functions, and triggers.
 - Direct test versions of your applications to the upgraded DB instance. Verify that the applications work correctly with the new version.

- Evaluate the storage used by the upgraded instance to determine if the upgrade requires additional storage. You might need to choose a larger instance class to support the new version in production. For more information, see [DB instance classes \(p. 10\)](#).
8. If all tests pass, upgrade your production DB instance. We recommend that you confirm that the DB instance working correctly before allowing write operations to the DB instance.

Upgrading an Oracle DB instance

To learn how to upgrade an Oracle DB instance, see [Upgrading a DB instance engine version \(p. 360\)](#).

Upgrading an Oracle DB snapshot

If you have existing manual DB snapshots, you can upgrade them to a later version of the Oracle database engine.

When Oracle stops providing patches for a version, and Amazon RDS deprecates the version, you can upgrade your snapshots that correspond to the deprecated version. For more information, see [Oracle engine version management \(p. 1758\)](#).

Amazon RDS supports upgrading snapshots in all AWS Regions.

Console

To upgrade an Oracle DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**, and then select the DB snapshot that you want to upgrade.
3. For **Actions**, choose **Upgrade snapshot**. The **Upgrade snapshot** page appears.
4. Choose the **New engine version** to upgrade the snapshot to.
5. (Optional) For **Option group**, choose the option group for the upgraded DB snapshot. The same option group considerations apply when upgrading a DB snapshot as when upgrading a DB instance. For more information, see [Option group considerations \(p. 1761\)](#).
6. Choose **Save changes** to save your changes.

During the upgrade process, all snapshot actions are disabled for this DB snapshot. Also, the DB snapshot status changes from **available** to **upgrading**, and then changes to **active** upon completion. If the DB snapshot can't be upgraded because of snapshot corruption issues, the status changes to **unavailable**. You can't recover the snapshot from this state.

Note

If the DB snapshot upgrade fails, the snapshot is rolled back to the original state with the original version.

AWS CLI

To upgrade an Oracle DB snapshot by using the AWS CLI, call the `modify-db-snapshot` command with the following parameters:

- `--db-snapshot-identifier` – The name of the DB snapshot.
- `--engine-version` – The version to upgrade the snapshot to.

You might also need to include the following parameter. The same option group considerations apply when upgrading a DB snapshot as when upgrading a DB instance. For more information, see [Option group considerations \(p. 1761\)](#).

- `--option-group-name` – The option group for the upgraded DB snapshot.

Example

The following example upgrades a DB snapshot.

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot \
--db-snapshot-identifier mydbsnapshot \
--engine-version 19.0.0.0.ru-2020-10.rur-2020-10.r1 \
--option-group-name default:oracle-se2-19
```

For Windows:

```
aws rds modify-db-snapshot ^
--db-snapshot-identifier mydbsnapshot ^
--engine-version 19.0.0.0.ru-2020-10.rur-2020-10.r1 ^
--option-group-name default:oracle-se2-19
```

RDS API

To upgrade an Oracle DB snapshot by using the Amazon RDS API, call the [ModifyDBSnapshot](#) operation with the following parameters:

- `DBSnapshotIdentifier` – The name of the DB snapshot.
- `EngineVersion` – The version to upgrade the snapshot to.

You might also need to include the `OptionGroupName` parameter. The same option group considerations apply when upgrading a DB snapshot as when upgrading a DB instance. For more information, see [Option group considerations \(p. 1761\)](#).

Using third-party software with your RDS for Oracle DB instance

To use tools and third-party software with RDS for Oracle DB instances, review the information in the following sections.

Topics

- [Setting up Amazon RDS to host tools and third-party software for Oracle \(p. 1767\)](#)
- [Using Oracle GoldenGate with Amazon RDS for Oracle \(p. 1773\)](#)
- [Using the Oracle Repository Creation Utility on RDS for Oracle \(p. 1786\)](#)
- [Configuring Oracle Connection Manager on an Amazon EC2 instance \(p. 1792\)](#)
- [Installing a Siebel database on Oracle on Amazon RDS \(p. 1794\)](#)

Setting up Amazon RDS to host tools and third-party software for Oracle

You can use Amazon RDS to host an Oracle DB instance that supports software and components such as the following:

- Siebel Customer Relationship Management (CRM)
- Oracle Fusion Middleware Metadata — installed by the Repository Creation Utility (RCU)

The following procedures help you create an Oracle DB instance on Amazon RDS that you can use to host additional software and components for Oracle.

Topics

- [Creating a VPC for use with an Oracle database \(p. 1767\)](#)
- [Creating an Oracle DB instance \(p. 1772\)](#)
- [Additional Amazon RDS interfaces \(p. 1772\)](#)

Creating a VPC for use with an Oracle database

In the following procedure, you create a virtual private cloud (VPC) based on the Amazon VPC service, a private subnet, and a security group. Your Amazon RDS DB instance needs to be available only to your middle-tier components, and not to the public internet. Thus, your Amazon RDS DB instance is hosted in a private subnet, providing greater security.

To create a VPC based on Amazon VPC

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, choose the AWS Region for your VPC. This example uses the US West (Oregon) region.
3. In the upper-left corner, choose **VPC Dashboard**, and then choose **Start VPC Wizard**.
4. On the page **Step 1: Select a VPC Configuration**, choose **VPC with Public and Private Subnets**, and then choose **Select**.
5. On the page **Step 2: VPC with Public and Private Subnets**, shown following, set the following values.

Option	Value
IPv4 CIDR block	10.0.0.0/16 For more information about selecting CIDR blocks for your VPC, see VPC sizing .
IPv6 CIDR block	No IPv6 CIDR Block
VPC name	The name for your VPC, for example vpc-1 .
Public subnet's IPv4 CIDR	10.0.0.0/24 For more information about subnet sizing, see Subnet sizing .
Availability Zone	An Availability Zone for your AWS Region.

Option	Value
Public subnet name	The name for your public subnet, for example subnet-public-1 .
Private subnet's IPv4 CIDR	10.0.1.0/24 For more information about subnet sizing, see Subnet sizing .
Availability Zone	An Availability Zone for your AWS Region.
Private subnet name	The name for your private subnet, for example subnet-private-1 .
Instance type	An instance type for your NAT instance, for example t2.small . Note If you don't see Instance type in the console, choose Use a NAT instance instead .
Key pair name	No key pair
Service endpoints	None
Enable DNS hostnames	Yes
Hardware tenancy	Default

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block: <input type="text" value="10.0.0.0/16"/>	(65531 IP addresses available)
IPv6 CIDR block:	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block
VPC name:	<input type="text" value="vpc-1"/>
Public subnet's IPv4 CIDR: <input type="text" value="10.0.0.0/24"/>	(251 IP addresses available)
Availability Zone: <input type="text" value="us-west-2a"/>	
Public subnet name:	<input type="text" value="subnet-public-1"/>
Private subnet's IPv4 CIDR: <input type="text" value="10.0.1.0/24"/>	(251 IP addresses available)
Availability Zone: <input type="text" value="us-west-2a"/>	
Private subnet name:	<input type="text" value="subnet-private-1"/>
You can add more subnets after AWS creates the VPC.	
Specify the details of your NAT instance (Instance rates apply). Use a NAT gateway instead	
Instance type: <input type="text" value="t2.small"/>	
Key pair name: <input type="text" value="No key pair"/>	
Service endpoints	
<input type="button" value="Add Endpoint"/>	
Enable DNS hostnames: <input checked="" type="radio"/> Yes <input type="radio"/> No	
Hardware tenancy: <input type="text" value="Default"/>	
<input type="button" value="Cancel and Exit"/> <input type="button" value="Back"/> <input style="background-color: #0070C0; color: white; font-weight: bold;" type="button" value="Create VPC"/>	

6. Choose **Create VPC**.

An Amazon RDS DB instance in a VPC requires at least two private subnets or at least two public subnets, to support Multi-AZ deployment. For more information about working with multiple Availability Zones, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#). Because your database is private, add a second private subnet to your VPC.

To create an additional subnet

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, confirm that you are in the correct AWS Region for your VPC.
3. In the upper-left corner, choose **VPC Dashboard**, choose **Subnets**, and then choose **Create Subnet**.

4. On the **Create Subnet** page, set the following values.

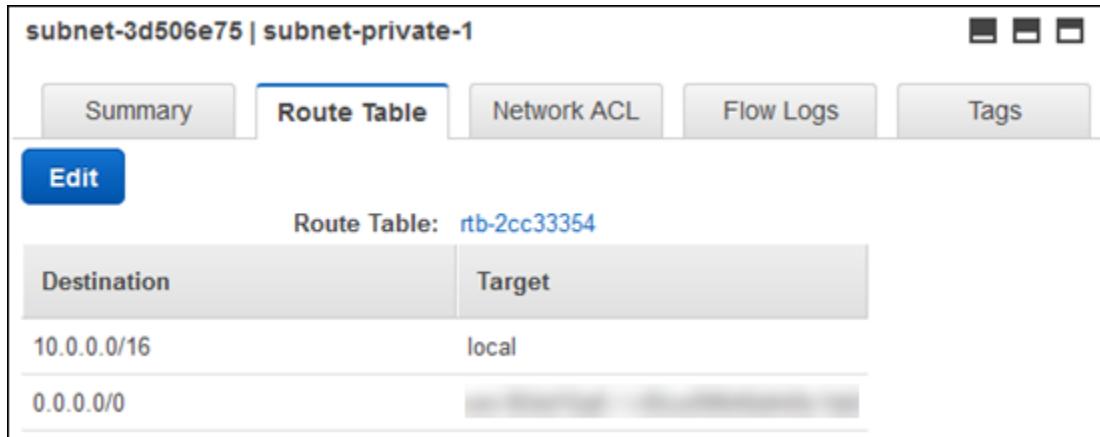
Option	Value
Name tag	The name for your second private subnet, for example subnet-private-2 .
VPC	Your VPC, for example vpc-1 .
Availability Zone	An Availability Zone for your AWS Region. Note Choose an Availability Zone different from the one that you chose for the first private subnet.
CIDR block	10.0.2.0/24

5. Choose **Yes, Create**.

Both private subnets must use the same route table. In the following procedure, you check to make sure the route tables match, and if not you edit one of them.

To ensure the subnets use the same route table.

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, confirm that you are in the correct AWS Region for your VPC.
3. In the upper-left corner, choose **VPC Dashboard**, choose **Subnets**, and then choose your first private subnet, for example **subnet-private-1**.
4. At the bottom of the console, choose the **Route Table** tab, shown following.



5. Make a note of the route table, for example **rtb-0d9fc668**.
6. In the list of subnets, choose the second private subnet, for example **subnet-private-2**.
7. At the bottom of the console, choose the **Route Table** tab.
8. If the route table for the second subnet is not the same as the route table for the first subnet, edit it to match:
 - a. Choose **Edit**.
 - b. For **Change to**, choose the route table that matches your first subnet.
 - c. Choose **Save**.

A security group acts as a virtual firewall for your DB instance to control inbound and outbound traffic. In the following procedure, you create a security group for your DB instance. For more information about security groups, see [Security groups for your VPC](#).

To create a VPC security group for a private Amazon RDS DB instance

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, confirm that you are in the correct AWS Region for your VPC.
3. In the upper-left corner, choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create Security Group**.
4. On the page **Create Security Group**, set the following values.

Option	Value
Name tag	The name for your security group, for example sgdb-1 .
Group name	The name for your security group, for example sgdb-1 .
Description	A description for your security group.
VPC	Your VPC, for example vpc-1 .

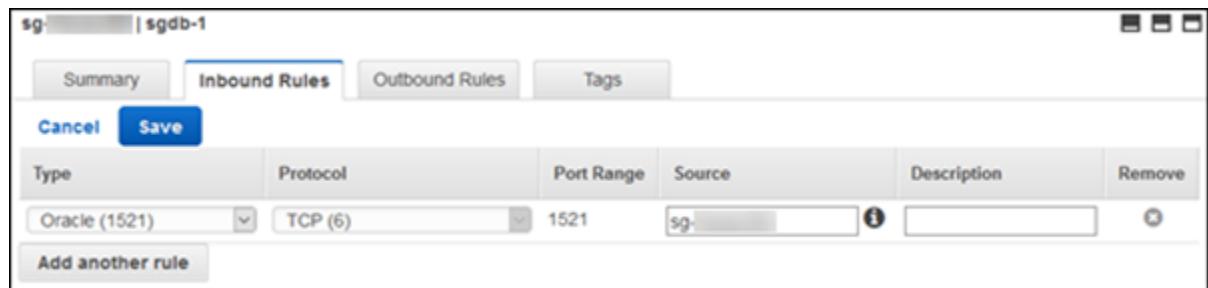
5. Choose **Yes, Create**.

In the following procedure, you add rules to your security group to control inbound traffic to your DB instance. For more information about inbound rules, see [Security group rules](#).

To add inbound rules to the security group

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, confirm that you are in the correct AWS Region for your VPC.
3. In the upper-left corner, choose **VPC Dashboard**, choose **Security Groups**, and then choose your security group, for example **sgdb-1**.
4. At the bottom of the console, choose the **Inbound Rules** tab, and then choose **Edit**.
5. Set these values, as shown following.

Option	Value
Type	Oracle (1521)
Protocol	TCP (6)
Port Range	1521
Source	The identifier of your security group. When you choose the box, you see the name of your security group, for example sgdb-1 .



6. Choose **Save**.

Creating an Oracle DB instance

You can use Amazon RDS to host an Oracle DB instance. When you create the new DB instance, specify the VPC and security group you created previously using the instructions in [Creating a VPC for use with an Oracle database \(p. 1767\)](#). Also, choose **No** for **Publicly accessible**.

For information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Additional Amazon RDS interfaces

In the preceding tasks, you use the AWS Management Console to perform tasks. Amazon Web Services also provides the AWS Command Line Interface (AWS CLI), and an application programming interface (API). You can use the AWS CLI or the API to automate many of the tasks for managing Amazon RDS, including tasks to manage an Oracle DB instance with Amazon RDS.

For more information, see [AWS Command Line Interface reference for Amazon RDS](#) and [Amazon RDS API Reference](#).

Using Oracle GoldenGate with Amazon RDS for Oracle

Oracle GoldenGate collects, replicates, and manages transactional data between databases. It is a log-based change data capture (CDC) and replication software package used with databases for online transaction processing (OLTP) systems. Oracle GoldenGate creates trail files that contain the most recent changed data from the source database. It then pushes these files to the server, where a process converts the trail file into standard SQL to be applied to the target database.

Oracle GoldenGate with RDS for Oracle supports the following features:

- Active-Active database replication
- Disaster recovery
- Data protection
- In-Region and cross-Region replication
- Zero-downtime migration and upgrades
- Data replication between an RDS for Oracle DB instance and a non-Oracle database

Note

For a list of supported databases, see [Oracle Fusion Middleware Supported System Configurations](#) in the Oracle documentation.

You can use Oracle GoldenGate with RDS for Oracle to upgrade to major versions of Oracle Database. For example, you can use Oracle GoldenGate to upgrade from an Oracle Database 11g on-premises database to Oracle Database 19c on an Amazon RDS DB instance.

Topics

- [Supported versions and licensing options for Oracle GoldenGate \(p. 1773\)](#)
- [Requirements and limitations for Oracle GoldenGate \(p. 1774\)](#)
- [Oracle GoldenGate architecture \(p. 1774\)](#)
- [Setting up Oracle GoldenGate \(p. 1777\)](#)
- [Working with the EXTRACT and REPLICAT utilities of Oracle GoldenGate \(p. 1782\)](#)
- [Troubleshooting Oracle GoldenGate \(p. 1784\)](#)

Supported versions and licensing options for Oracle GoldenGate

You can use Standard Edition Two (SE2) or Enterprise Edition (EE) of RDS for Oracle with Oracle GoldenGate version 12c and higher. You can use the following Oracle GoldenGate features:

- Oracle GoldenGate Remote Capture (extract) is supported.
- Capture (extract) is supported on RDS for Oracle DB instances that use the traditional non-CDB database architecture. Oracle GoldenGate Remote PDB capture is supported on Oracle Database 21c container databases (CDBs).
- Oracle GoldenGate Remote Delivery (replicat) is supported on RDS for Oracle DB instances that use either the non-CDB or CDB architectures. Remote Delivery supports Integrated Replicat, Parallel Replicat, Coordinated Replicat, and classic Replicat.
- RDS for Oracle supports the Classic and Microservices architectures of Oracle GoldenGate.
- Oracle GoldenGate DDL and Sequence value replication is supported when using Integrated capture mode.

You are responsible for managing Oracle GoldenGate licensing (BYOL) for use with Amazon RDS in all AWS Regions. For more information, see [RDS for Oracle licensing options \(p. 1474\)](#).

Requirements and limitations for Oracle GoldenGate

When you're working with Oracle GoldenGate and RDS for Oracle, consider the following requirements and limitations:

- You're responsible for setting up and managing Oracle GoldenGate for use with RDS for Oracle.
- You're responsible for setting up an Oracle GoldenGate version that is certified with the source and the target databases. For more information, see [Oracle Fusion Middleware Supported System Configurations](#) in the Oracle documentation.
- You can use Oracle GoldenGate on many different AWS environments for many different use cases. If you have a support-related issue relating to Oracle GoldenGate, contact Oracle Support Services.
- You can use Oracle GoldenGate on RDS for Oracle DB instances that use Oracle Transparent Data Encryption (TDE). To maintain the integrity of replicated data, configure encryption on the Oracle GoldenGate hub using Amazon EBS encrypted volumes or trail file encryption. Also configure encryption for data sent between the Oracle GoldenGate hub and the source and target database instances. RDS for Oracle DB instances support encryption with [Oracle Secure Sockets Layer \(p. 1722\)](#) or [Oracle native network encryption \(p. 1711\)](#).

Oracle GoldenGate architecture

The Oracle GoldenGate architecture for use with Amazon RDS consists of the following decoupled modules:

Source database

Your source database can be either an on-premises Oracle database, an Oracle database on an Amazon EC2 instance, or an Oracle database on an Amazon RDS DB instance.

Oracle GoldenGate hub

An Oracle GoldenGate hub moves transaction information from the source database to the target database. Your hub can be either of the following:

- An Amazon EC2 instance with Oracle Database and Oracle GoldenGate installed
- An on-premises Oracle installation

You can have more than one Amazon EC2 hub. We recommend that you use two hubs if you use Oracle GoldenGate for cross-Region replication.

Target database

Your target database can be on either an Amazon RDS DB instance, an Amazon EC2 instance, or an on-premises location.

The following sections describe common scenarios for Oracle GoldenGate on Amazon RDS.

Topics

- [On-premises source database and Oracle GoldenGate hub \(p. 1775\)](#)
- [On-premises source database and Amazon EC2 hub \(p. 1775\)](#)
- [Amazon RDS source database and Amazon EC2 hub \(p. 1775\)](#)
- [Amazon EC2 source database and Amazon EC2 hub \(p. 1776\)](#)
- [Amazon EC2 hubs in different AWS Regions \(p. 1776\)](#)

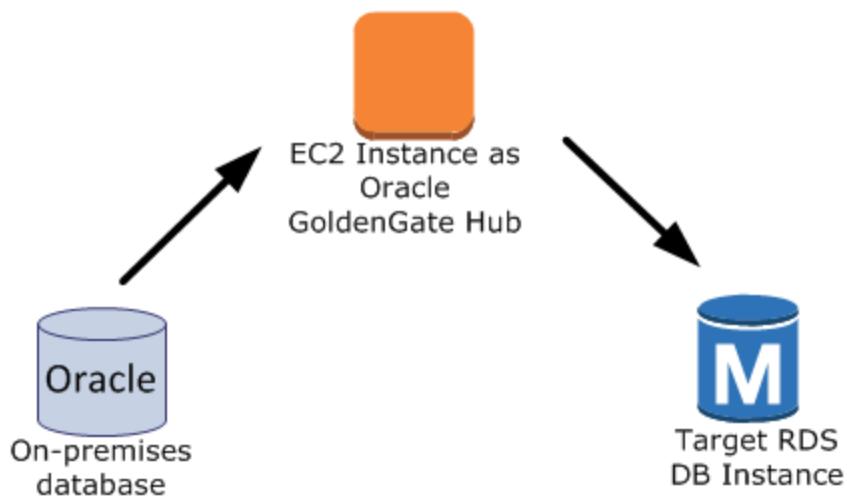
On-premises source database and Oracle GoldenGate hub

In this scenario, an on-premises Oracle source database and on-premises Oracle GoldenGate hub provides data to a target Amazon RDS DB instance.



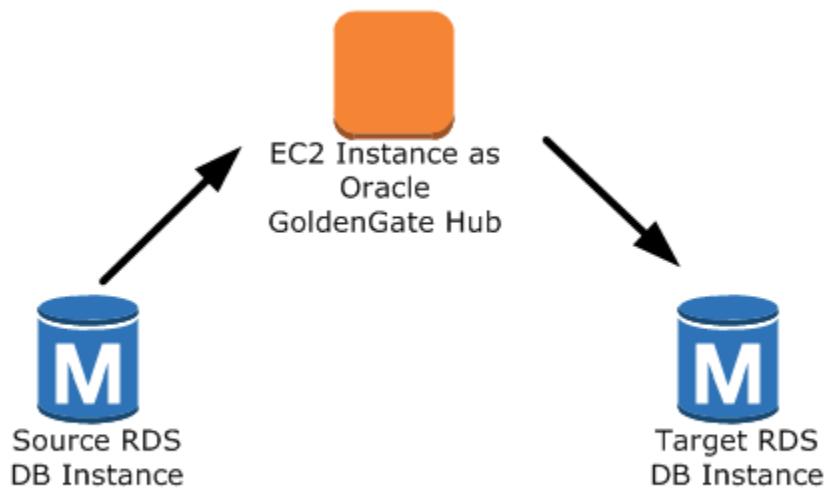
On-premises source database and Amazon EC2 hub

In this scenario, an on-premises Oracle database acts as the source database. It's connected to an Amazon EC2 instance hub. This hub provides data to a target RDS for Oracle DB instance.



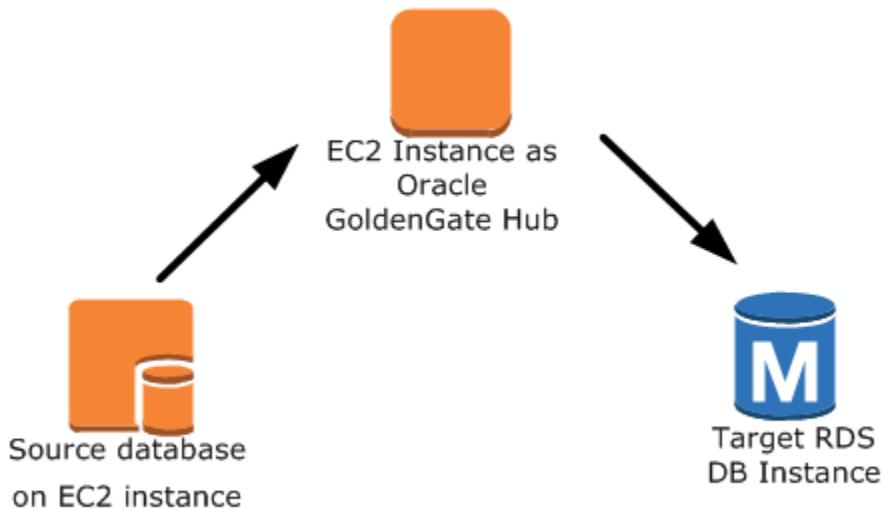
Amazon RDS source database and Amazon EC2 hub

In this scenario, an RDS for Oracle DB instance acts as the source database. It's connected to an Amazon EC2 instance hub. This hub provides data to a target RDS for Oracle DB instance.



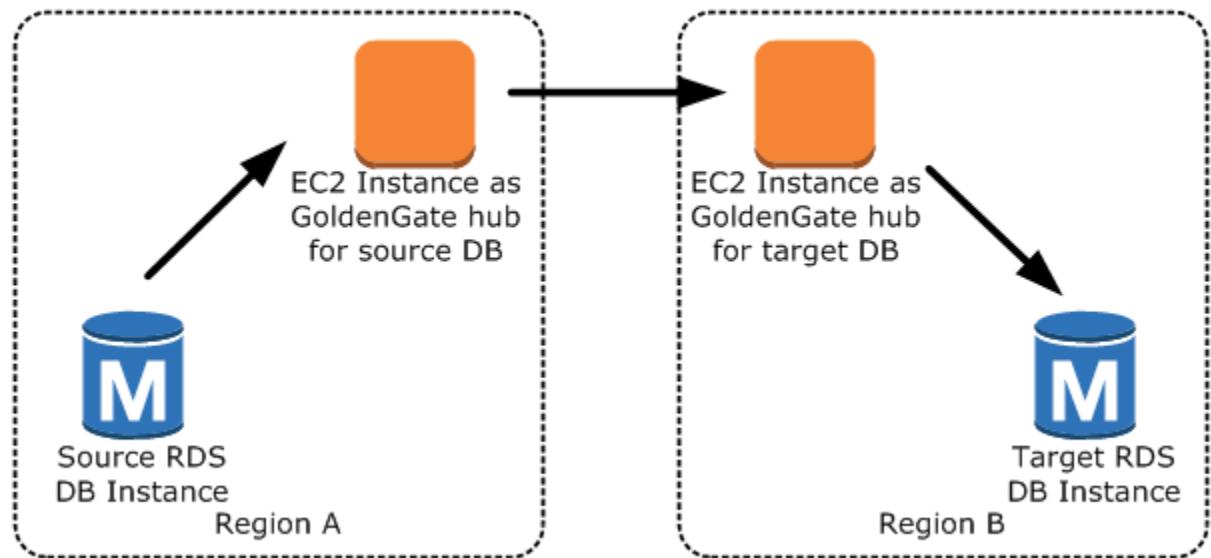
Amazon EC2 source database and Amazon EC2 hub

In this scenario, an Oracle database on an Amazon EC2 instance acts as the source database. It's connected to an Amazon EC2 instance hub. This hub provides data to a target RDS for Oracle DB instance.



Amazon EC2 hubs in different AWS Regions

In this scenario, an Oracle database on an Amazon RDS DB instance is connected to an Amazon EC2 instance hub in the same AWS Region. The hub is connected to an Amazon EC2 instance hub in a different AWS Region. This second hub provides data to the target RDS for Oracle DB instance in the same AWS Region as the second Amazon EC2 instance hub.



Note

Any issues that affect running Oracle GoldenGate on an on-premises environment also affect running Oracle GoldenGate on AWS. We strongly recommend that you monitor the Oracle GoldenGate hub to ensure that EXTRACT and REPLICAT are resumed if a failover occurs.

Because the Oracle GoldenGate hub is run on an Amazon EC2 instance, Amazon RDS does not manage the Oracle GoldenGate hub and cannot ensure that it is running.

Setting up Oracle GoldenGate

To set up Oracle GoldenGate using Amazon RDS, configure the hub on an Amazon EC2 instance, and then configure the source and target databases. The following sections give an example of how to set up Oracle GoldenGate for use with Amazon RDS for Oracle.

Topics

- [Setting up an Oracle GoldenGate hub on Amazon EC2 \(p. 1777\)](#)
- [Setting up a source database for use with Oracle GoldenGate on Amazon RDS \(p. 1778\)](#)
- [Setting up a target database for use with Oracle GoldenGate on Amazon RDS \(p. 1780\)](#)

Setting up an Oracle GoldenGate hub on Amazon EC2

To create an Oracle GoldenGate hub on an Amazon EC2 instance, you first create an Amazon EC2 instance with a full client installation of Oracle RDBMS. The Amazon EC2 instance must also have Oracle GoldenGate software installed. The Oracle GoldenGate software versions depend on the source and target database versions. For more information about installing Oracle GoldenGate, see the [Oracle GoldenGate documentation](#).

The Amazon EC2 instance that serves as the Oracle GoldenGate hub stores and processes the transaction information from the source database into trail files. To support this process, make sure that you meet the following requirements:

- You have allocated enough storage for the trail files.
- The Amazon EC2 instance has enough processing power to manage the amount of data.
- The EC2 instance has enough memory to store the transaction information before it's written to the trail file.

To set up an Oracle GoldenGate classic architecture hub on an Amazon EC2 instance

1. Create subdirectories in the Oracle GoldenGate directory.

In the Amazon EC2 command line shell, start `ggsci`, the Oracle GoldenGate command interpreter. The `CREATE SUBDIRS` command creates subdirectories under the `/gg` directory for parameter, report, and checkpoint files.

```
prompt$ cd /gg
prompt$ ./ggsci

GGSCI> CREATE SUBDIRS
```

2. Configure the `mgr.prm` file.

The following example adds lines to the `$GGHOME/dirprm/mgr.prm` file.

```
PORT 8199
PurgeOldExtracts ./dirdat/*, UseCheckpoints, MINKEEPDAYS 5
```

3. Start the manager.

The following example starts `ggsci` and runs the `start mgr` command.

```
GGSCI> start mgr
```

The Oracle GoldenGate hub is now ready for use.

Setting up a source database for use with Oracle GoldenGate on Amazon RDS

When your source database is running Oracle Database 12c or later, complete the following tasks to set up a source database for use with Oracle GoldenGate.

Setup steps

- [Step 1: Turn on supplemental logging on the source database \(p. 1778\)](#)
- [Step 2: Set the ENABLE_GOLDENGATE_REPLICATION initialization parameter to true \(p. 1778\)](#)
- [Step 3: Set the log retention period on the source database \(p. 1779\)](#)
- [Step 4: Create an Oracle GoldenGate user account on the source database \(p. 1779\)](#)
- [Step 5: Grant user account privileges on the source database \(p. 1779\)](#)
- [Step 6: Add a TNS alias for the source database \(p. 1780\)](#)

Step 1: Turn on supplemental logging on the source database

To turn on the minimum database-level supplemental logging, run the following PL/SQL procedure:

```
EXEC rdsadmin.rdsadmin_util.alter_supplemental_logging(p_action => 'ADD')
```

Step 2: Set the ENABLE_GOLDENGATE_REPLICATION initialization parameter to true

When you set the `ENABLE_GOLDENGATE_REPLICATION` initialization parameter to `true`, it allows database services to support logical replication. If your source database is on an Amazon RDS DB instance, make sure that you have a parameter group assigned to the DB instance with the `ENABLE_GOLDENGATE_REPLICATION` initialization parameter set to `true`. For more information about the `ENABLE_GOLDENGATE_REPLICATION` initialization parameter, see the [Oracle Database documentation](#).

Step 3: Set the log retention period on the source database

Make sure that you configure the source database to retain archived redo logs. Consider the following guidelines:

- Specify the duration for log retention in hours. The minimum value is one hour.
- Set the duration to exceed any potential downtime of the source DB instance, any potential period of communication, and any potential period of networking issues for the source instance. Such a duration lets Oracle GoldenGate recover logs from the source instance as needed.
- Ensure that you have sufficient storage on your instance for the files.

For example, set the retention period for archived redo logs to 24 hours.

```
EXEC rdsadmin.rdsadmin_util.set_configuration('archivelog retention hours',24)
```

If you don't have log retention enabled, or if the retention value is too small, you receive an error message similar to the following.

```
2022-03-06 06:17:27  ERROR  OGG-00446  error 2 (No such file or directory)
opening redo log /rdsdbdata/db/GGTEST3_A/onlinelog/o1_mf_2_9k4bp1n6_.log for sequence 1306
Not able to establish initial position for begin time 2022-03-06 06:16:55.
```

Because your DB instance retains your archived redo logs, make sure that you have sufficient space for the files. To see how much space you have used in the last *num_hours* hours, run the following query, replacing *num_hours* with the number of hours.

```
SELECT SUM(BLOCKS * BLOCK_SIZE) BYTES FROM V$ARCHIVED_LOG
WHERE NEXT_TIME>=SYSDATE-num_hours/24 AND DEST_ID=1;
```

Step 4: Create an Oracle GoldenGate user account on the source database

Oracle GoldenGate runs as a database user and requires the appropriate database privileges to access the redo and archived redo logs for the source database. To provide these, create a user account on the source database. For more information about the permissions for an Oracle GoldenGate user account, see the [Oracle documentation](#).

The following statements create a user account named oggadm1.

```
CREATE TABLESPACE administrator;
CREATE USER oggadm1 IDENTIFIED BY "password"
  DEFAULT TABLESPACE ADMINISTRATOR TEMPORARY TABLESPACE TEMP;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator;
```

Step 5: Grant user account privileges on the source database

In this task, you grant necessary account privileges for database users on your source database.

To grant account privileges on the source database

1. Grant the necessary privileges to the Oracle GoldenGate user account using the SQL command `grant` and the `rdsadmin.rdsadmin_util` procedure `grant_sys_object`. The following statements grant privileges to a user named oggadm1.

```
GRANT CREATE SESSION, ALTER SESSION TO oggadm1;
GRANT RESOURCE TO oggadm1;
GRANT SELECT ANY DICTIONARY TO oggadm1;
```

```
GRANT FLASHBACK ANY TABLE TO oggadm1;
GRANT SELECT ANY TABLE TO oggadm1;
GRANT SELECT_CATALOG_ROLE TO rds_master_user_name WITH ADMIN OPTION;
EXEC rdsadmin.rdsadmin_util.grant_sys_object ('DBA_CLUSTERS', 'OGGADM1');
GRANT EXECUTE ON DBMS_FLASHBACK TO oggadm1;
GRANT SELECT ON SYS.V_$DATABASE TO oggadm1;
GRANT ALTER ANY TABLE TO oggadm1;
```

2. Grant the privileges needed by a user account to be an Oracle GoldenGate administrator.

The package that you use to perform the grant, dbms_goldengate_auth or rdsadmin_dbms_goldengate_auth, depends on the Oracle DB engine version.

- For Oracle DB versions that are later than or equal to Oracle Database 12c Release 2 (12.2), which requires patch level 12.2.0.1.ru-2019-04.rur-2019-04.r1 or later, run the following PL/SQL program.

```
EXEC rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (
    grantee              => 'OGGADM1',
    privilege_type       => 'capture',
    grant_select_privileges => true,
    do_grants            => TRUE);
```

- For Oracle database versions that are earlier than Oracle Database 12c Release 2 (12.2), run the following PL/SQL program.

```
EXEC dbms_goldengate_auth.grant_admin_privilege (
    grantee              => 'OGGADM1',
    privilege_type       => 'capture',
    grant_select_privileges => true,
    do_grants            => TRUE);
```

To revoke privileges, use the procedure `revoke_admin_privilege` in the same package.

Step 6: Add a TNS alias for the source database

Add the following entry to `$ORACLE_HOME/network/admin/tnsnames.ora` in the Oracle home to be used by the EXTRACT process. For more information on the `tnsnames.ora` file, see the [Oracle documentation](#).

```
OGGSOURCE=
  (DESCRIPTION=
    (ENABLE=BROKEN)
    (ADDRESS_LIST=
      (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-source.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
      (CONNECT_DATA=(SERVICE_NAME=ORCL))
    )
```

Setting up a target database for use with Oracle GoldenGate on Amazon RDS

In this task, you set up a target DB instance for use with Oracle GoldenGate.

Setup steps

- [Step 1: Set the ENABLE_GOLDENGATE_REPLICATION initialization parameter to true \(p. 1781\)](#)
- [Step 2: Create an Oracle GoldenGate user account on the target database \(p. 1781\)](#)
- [Step 3: Grant account privileges on the target database \(p. 1781\)](#)
- [Step 4: Add a TNS alias for the target database \(p. 1782\)](#)

Step 1: Set the ENABLE_GOLDENGATE_REPLICATION initialization parameter to true

When you set the ENABLE_GOLDENGATE_REPLICATION initialization parameter to true, it allows database services to support logical replication. If your source database is on an Amazon RDS DB instance, make sure that you have a parameter group assigned to the DB instance with the ENABLE_GOLDENGATE_REPLICATION initialization parameter set to true. For more information about the ENABLE_GOLDENGATE_REPLICATION initialization parameter, see the [Oracle Database documentation](#).

Step 2: Create an Oracle GoldenGate user account on the target database

Oracle GoldenGate runs as a database user and requires the appropriate database privileges. To make sure it has these privileges, create a user account on the target database.

The following statement creates a user named oggadm1.

```
CREATE TABLESPSACE administrator;
CREATE USER oggadm1 IDENTIFIED BY "password"
    DEFAULT TABLESPACE administrator
    TEMPORARY TABLESPACE temp;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator;
```

Step 3: Grant account privileges on the target database

In this task, you grant necessary account privileges for database users on your target database.

To grant account privileges on the target database

- Grant necessary privileges to the Oracle GoldenGate user account on the target database. In the following example, you grant privileges to oggadm1.

```
GRANT CREATE SESSION      TO oggadm1;
GRANT ALTER SESSION       TO oggadm1;
GRANT CREATE CLUSTER      TO oggadm1;
GRANT CREATE INDEXTYPE    TO oggadm1;
GRANT CREATE OPERATOR     TO oggadm1;
GRANT CREATE PROCEDURE    TO oggadm1;
GRANT CREATE SEQUENCE     TO oggadm1;
GRANT CREATE TABLE        TO oggadm1;
GRANT CREATE TRIGGER      TO oggadm1;
GRANT CREATE TYPE         TO oggadm1;
GRANT SELECT ANY DICTIONARY TO oggadm1;
GRANT CREATE ANY TABLE    TO oggadm1;
GRANT ALTER ANY TABLE     TO oggadm1;
GRANT LOCK ANY TABLE      TO oggadm1;
GRANT SELECT ANY TABLE    TO oggadm1;
GRANT INSERT ANY TABLE    TO oggadm1;
GRANT UPDATE ANY TABLE    TO oggadm1;
GRANT DELETE ANY TABLE    TO oggadm1;
```

- Grant the privileges needed by a user account to be an Oracle GoldenGate administrator. The package that you use to perform the grant, dbms_goldengate_auth or rdsadmin_dbms_goldengate_auth, depends on the Oracle DB engine version.

- For Oracle database versions that are later than or equal to Oracle Database 12c Release 2 (12.2), which requires patch level 12.2.0.1.ru-2019-04.rur-2019-04.r1 or later, run the following PL/SQL program.

```
EXEC rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (
    grantee           => 'OGGADM1',
```

```
privilege_type      => 'apply',
grant_select_privileges => true,
do_grants           => TRUE);
```

- For Oracle database versions that are lower than Oracle Database 12c Release 2 (12.2), run the following PL/SQL program.

```
EXEC dbms_goldengate_auth.grant_admin_privilege (
    grantee              => 'OGGADM1',
    privilege_type        => 'apply',
    grant_select_privileges => true,
    do_grants             => TRUE);
```

To revoke privileges, use the procedure `revoke_admin_privilege` in the same package.

Step 4: Add a TNS alias for the target database

Add the following entry to `$ORACLE_HOME/network/admin/tnsnames.ora` in the Oracle home to be used by the REPLICAT process. For Oracle Multitenant databases, make sure that the TNS alias points to the service name of the PDB. For more information on the `tnsnames.ora` file, see the [Oracle documentation](#).

```
OGGTARGET=
  (DESCRIPTION=
    (ENABLE=BROKEN)
    (ADDRESS_LIST=
      (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-target.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
    (CONNECT_DATA=(SERVICE_NAME=ORCL))
  )
```

Working with the EXTRACT and REPLICAT utilities of Oracle GoldenGate

The Oracle GoldenGate utilities EXTRACT and REPLICAT work together to keep the source and target databases in sync via incremental transaction replication using trail files. All changes that occur on the source database are automatically detected by EXTRACT, then formatted and transferred to trail files on the Oracle GoldenGate on-premises or EC2-instance hub. After initial load is completed, the data is read from these files and replicated to the target database by the REPLICAT utility.

Running the Oracle GoldenGate EXTRACT utility

The EXTRACT utility retrieves, converts, and outputs data from the source database to trail files. EXTRACT queues transaction details to memory or to temporary disk storage. When the transaction is committed to the source database, EXTRACT flushes all of the transaction details to a trail file. The trail file routes these details to the Oracle GoldenGate on-premises or the Amazon EC2 instance hub and then to the target database.

The following steps start the EXTRACT utility, capture the data from EXAMPLE.TABLE in source database OGGSOURCE, and create the trail files.

To run the EXTRACT utility

- Configure the EXTRACT parameter file on the Oracle GoldenGate hub (on-premises or Amazon EC2 instance). The following listing shows an example EXTRACT parameter file named `$GGHOME/diirprm/eabc.prm`.

```
EXTRACT EABC

USERID oggadm1@OGGSOURCE, PASSWORD "my-password"
EXTTRAIL /path/to/goldengate/dirdat/ab

IGNOREREPLICATES
GETAPLOPS
TRANLOGOPTIONS EXCLUDEUSER OGGADM1

TABLE EXAMPLE.TABLE;
```

2. On the Oracle GoldenGate hub, log in to the source database and launch the Oracle GoldenGate command line interface ggsci. The following example shows the format for logging in.

```
dblogin oggadm1@OGGSOURCE
```

3. Add transaction data to turn on supplemental logging for the database table.

```
add trandata EXAMPLE.TABLE
```

4. Using the ggsci command line, enable the EXTRACT utility using the following commands.

```
add extract EABC tranlog, INTEGRATED tranlog, begin now
add exttrail /path/to/goldengate/dirdat/ab
extract EABC,
MEGABYTES 100
```

5. Register the EXTRACT utility with the database so that the archive logs are not deleted. This task allows you to recover old, uncommitted transactions if necessary. To register the EXTRACT utility with the database, use the following command.

```
register EXTRACT EABC, DATABASE
```

6. Start the EXTRACT utility with the following command.

```
start EABC
```

Running the Oracle GoldenGate REPLICAT utility

The REPLICAT utility "pushes" transaction information in the trail files to the target database.

The following steps enable and start the REPLICAT utility so that it can replicate the captured data to the table EXAMPLE . TABLE in target database OGGTARGET.

To run the REPLICATE utility

1. Configure the REPLICAT parameter file on the Oracle GoldenGate hub (on-premises or EC2 instance). The following listing shows an example REPLICAT parameter file named \$GGHOME/ dirprm/rabc.prm.

```
REPLICAT RABC

USERID oggadm1@OGGTARGET, password "my-password"

ASSUMETARGETDEFS
MAP EXAMPLE.TABLE, TARGET EXAMPLE.TABLE;
```

2. Log in to the target database and launch the Oracle GoldenGate command line interface (ggsci). The following example shows the format for logging in.

```
dblogin userid oggadm1@OGGTARGET
```

3. Using the ggsci command line, add a checkpoint table. The user indicated should be the Oracle GoldenGate user account, not the target table schema owner. The following example creates a checkpoint table named gg_checkpoint.

```
add checkpointtable oggadm1.oggchkpt
```

4. To enable the REPLICAT utility, use the following command.

```
add replicat RABC EXTTRAIL /path/to/goldengate/dirdat/ab CHECKPOINTTABLE  
oggadm1.oggchkpt
```

5. Start the REPLICAT utility by using the following command.

```
start RABC
```

Troubleshooting Oracle GoldenGate

This section explains the most common issues when using Oracle GoldenGate with Amazon RDS for Oracle.

Topics

- [Error opening an online redo log \(p. 1784\)](#)
- [Oracle GoldenGate appears to be properly configured but replication is not working \(p. 1784\)](#)
- [Integrated REPLICAT slow due to query on SYS."_DBA_APPLY_CDR_INFO" \(p. 1785\)](#)

Error opening an online redo log

Make sure that you configure your databases to retain archived redo logs. Consider the following guidelines:

- Specify the duration for log retention in hours. The minimum value is one hour.
- Set the duration to exceed any potential downtime of the source DB instance, any potential period of communication, and any potential period of networking issues for the source DB instance. Such a duration lets Oracle GoldenGate recover logs from the source DB instance as needed.
- Ensure that you have sufficient storage on your instance for the files.

If you don't have log retention enabled, or if the retention value is too small, you receive an error message similar to the following.

```
2022-03-06 06:17:27  ERROR  OGG-00446  error 2 (No such file or directory)  
opening redo log /rdsbdbdata/db/GGTEST3_A/onlinelog/o1_mf_2_9k4bp1n6_.log for sequence 1306  
Not able to establish initial position for begin time 2022-03-06 06:16:55.
```

Oracle GoldenGate appears to be properly configured but replication is not working

For pre-existing tables, you must specify the SCN that Oracle GoldenGate works from.

To fix this issue

1. Log in to the source database and launch the Oracle GoldenGate command line interface (ggsci). The following example shows the format for logging in.

```
dblogin userid oggadm1@OGGSOURCE
```

2. Using the ggsci command line, set up the start SCN for the EXTRACT process. The following example sets the SCN to 223274 for the EXTRACT.

```
ALTER EXTRACT EABC SCN 223274
start EABC
```

3. Log in to the target database. The following example shows the format for logging in.

```
dblogin userid oggadm1@OGGTARGET
```

4. Using the ggsci command line, set up the start SCN for the REPLICAT process. The following example sets the SCN to 223274 for the REPLICAT.

```
start RABC atcsn 223274
```

Integrated REPLICAT slow due to query on SYS."_DBA_APPLY_CDR_INFO"

Oracle GoldenGate Conflict Detection and Resolution (CDR) provides basic conflict resolution routines. For example, CDR can resolve a unique conflict for an INSERT statement.

When CDR resolves a collision, it can insert records into the exception table _DBA_APPLY_CDR_INFO temporarily. Integrated REPLICAT deletes these records later. In a rare scenario, the integrated REPLICAT can process a large number of collisions, but a new integrated REPLICAT does not replace it. Instead of being removed, the existing rows in _DBA_APPLY_CDR_INFO are orphaned. Any new integrated REPLICAT processes slow down because they are querying orphaned rows in _DBA_APPLY_CDR_INFO.

To remove all rows from _DBA_APPLY_CDR_INFO, use the Amazon RDS procedure `rdsadmin.rdsadmin_util.truncate_apply$_cdr_info`. This procedure is released as part of the October 2020 release and patch update. The procedure is available in the following database versions:

- Version 21.0.0.0.ru-2022-01.rur-2022-01.r1 and higher
- Version 19.0.0.0.ru-2020-10.rur-2020-10.r1 and higher

The following example truncates the table _DBA_APPLY_CDR_INFO.

```
SET SERVEROUTPUT ON SIZE 2000
EXEC rdsadmin.rdsadmin_util.truncate_apply$_cdr_info;
```

Using the Oracle Repository Creation Utility on RDS for Oracle

You can use Amazon RDS to host an RDS for Oracle DB instance that holds the schemas to support your Oracle Fusion Middleware components. Before you can use Fusion Middleware components, create and populate schemas for them in your database. You create and populate the schemas by using the Oracle Repository Creation Utility (RCU).

Supported versions and licensing options for RCU

Amazon RDS supports Oracle Repository Creation Utility (RCU) version 12c only. You can use the RCU in the following configurations:

- RCU 12c with Oracle Database 21c
- RCU 12c with Oracle Database 19c
- RCU 12c with Oracle Database 12c Release 2 (12.2)
- RCU 12c with Oracle Database 12c Release 1 (12.1) using 12.1.0.2.v4 or higher

Before you can use RCU, make sure that you do the following:

- Obtain a license for Oracle Fusion Middleware.
- Follow the Oracle licensing guidelines for the Oracle database that hosts the repository. For more information, see [Oracle Fusion Middleware Licensing Information User Manual](#) in the Oracle documentation.

Fusion MiddleWare supports repositories on Oracle Database Enterprise Edition and Standard Edition Two. Oracle recommends Enterprise Edition for production installations that require partitioning and installations that require online index rebuild.

Before you create your RDS for Oracle instance, confirm the Oracle database version that you need to support the components that you want to deploy. To find the requirements for the Fusion Middleware components and versions you want to deploy, use the Certification Matrix. For more information, see [Oracle Fusion Middleware Supported System Configurations](#) in the Oracle documentation.

Amazon RDS supports Oracle database version upgrades as needed. For more information, see [Upgrading a DB instance engine version \(p. 360\)](#).

Requirements and limitations for RCU

To use RCU, you need an Amazon VPC. Your Amazon RDS DB instance must be available only to your Fusion Middleware components, and not to the public Internet. Thus, host your Amazon RDS DB instance in a private subnet, which provides greater security. For information about how to create an Amazon VPC for use with an RDS for Oracle instance, see [Creating a VPC for use with an Oracle database \(p. 1767\)](#).

You also need an RDS for Oracle DB instance. For information about how to create an RDS for Oracle DB instance for use with Fusion Middleware metadata, see [Creating an Oracle DB instance \(p. 1772\)](#).

You can store the schemas for any Fusion Middleware components in your Amazon RDS DB instance. The following schemas have been verified to install correctly:

- Analytics (ACTIVITIES)
- Audit Services (IAU)

- Audit Services Append (IAU_APPEND)
- Audit Services Viewer (IAU_VIEWER)
- Discussions (DISCUSSIONS)
- Metadata Services (MDS)
- Oracle Business Intelligence (BIPLATFORM)
- Oracle Platform Security Services (OPSS)
- Portal and Services (WEBCENTER)
- Portlet Producers (PORTLET)
- Service Table (STB)
- SOA Infrastructure (SOAINFRA)
- User Messaging Service (UCSUMS)
- WebLogic Services (WLS)

Guidelines for using RCU

The following are some recommendations for working with your DB instance in this scenario:

- We recommend that you use Multi-AZ for production workloads. For more information about working with multiple Availability Zones, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).
- For additional security, Oracle recommends that you use Transparent Data Encryption (TDE) to encrypt your data at rest. If you have an Enterprise Edition license that includes the Advanced Security Option, you can enable encryption at rest by using the TDE option. For more information, see [Oracle Transparent Data Encryption \(p. 1751\)](#).

Amazon RDS also provides an encryption at rest option for all database editions. For more information, see [Encrypting Amazon RDS resources \(p. 2000\)](#).

- Configure your VPC Security Groups to allow communication between your application servers and your Amazon RDS DB instance. The application servers that host the Fusion Middleware components can be on Amazon EC2 or on-premises.

Running RCU

To create and populate the schemas to support your Fusion Middleware components, use the Oracle Repository Creation Utility (RCU). You can run RCU in different ways.

Topics

- [Running RCU using the command line in one step \(p. 1787\)](#)
- [Running RCU using the command line in multiple steps \(p. 1788\)](#)
- [Running RCU in interactive mode \(p. 1789\)](#)

Running RCU using the command line in one step

If you don't need to edit any of your schemas before populating them, you can run RCU in a single step. Otherwise, see the following section for running RCU in multiple steps.

You can run the RCU in silent mode by using the command-line parameter `-silent`. When you run RCU in silent mode, you can avoid typing passwords on the command line by creating a text file containing the passwords. Create a text file with the password for `dbUser1` on the first line, and the password for each component on subsequent lines. You specify the name of the password file as the last parameter to the RCU command.

Example

The following example creates and populates schemas for the SOA Infrastructure component (and its dependencies) in a single step.

For Linux, macOS, or Unix:

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-createRepository \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-f < /tmp/passwordfile.txt
```

For more information, see [Running Repository Creation Utility from the command line](#) in the Oracle documentation.

Running RCU using the command line in multiple steps

To manually edit your schema scripts, run RCU in multiple steps:

1. Run RCU in **Prepare Scripts for System Load** mode by using the `-generateScript` command-line parameter to create the scripts for your schemas.
2. Manually edit and run the generated script `script_systemLoad.sql`.
3. Run RCU again in **Perform Product Load** mode by using the `-dataLoad` command-line parameter to populate the schemas.
4. Run the generated cleanup script `script_postDataLoad.sql`.

To run RCU in silent mode, specify the command-line parameter `-silent`. When you run RCU in silent mode, you can avoid typing passwords on the command line by creating a text file containing the passwords. Create a text file with the password for `dbUser` on the first line, and the password for each component on subsequent lines. Specify the name of the password file as the last parameter to the RCU command.

Example

The following example creates schema scripts for the SOA Infrastructure component and its dependencies.

For Linux, macOS, or Unix:

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-generateScript \
```

```
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
[-encryptTablespace true] \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-scriptLocation /tmp/rcuscripts \
-f < /tmp/passwordfile.txt
```

Now you can edit the generated script, connect to your Oracle DB instance, and run the script. The generated script is named `script_systemLoad.sql`. For information about connecting to your Oracle DB instance, see [Connecting to your sample Oracle DB instance \(p. 184\)](#).

The following example populates the schemas for the SOA Infrastructure component (and its dependencies).

For Linux, macOS, or Unix:

```
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-dataLoad \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-f < /tmp/passwordfile.txt
```

To finish, you connect to your Oracle DB instance, and run the clean-up script. The script is named `script_postDataLoad.sql`.

For more information, see [Running Repository Creation Utility from the command line](#) in the Oracle documentation.

Running RCU in interactive mode

To use the RCU graphical user interface, run RCU in interactive mode. Include the `-interactive` parameter and omit the `-silent` parameter. For more information, see [Understanding Repository Creation Utility screens](#) in the Oracle documentation.

Example

The following example starts RCU in interactive mode and pre-populates the connection information.

For Linux, macOS, or Unix:

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-interactive \
-createRepository \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal
```

Troubleshooting RCU

Be mindful of the following issues.

Topics

- [Oracle Managed Files \(OMF\) \(p. 1790\)](#)
- [Object privileges \(p. 1790\)](#)
- [Enterprise Scheduler Service \(p. 1791\)](#)

Oracle Managed Files (OMF)

Amazon RDS uses OMF data files to simplify storage management. You can customize tablespace attributes, such as size and extent management. However, if you specify a data file name when you run RCU, the tablespace code fails with ORA-20900. You can use RCU with OMF in the following ways:

- In RCU 12.2.1.0 and later, use the `-honorOMF` command-line parameter.
- In RCU 12.1.0.3 and later, use multiple steps and edit the generated script. For more information, see [Running RCU using the command line in multiple steps \(p. 1788\)](#).

Object privileges

Because Amazon RDS is a managed service, you don't have full SYSDBA access to your RDS for Oracle DB instance. However, RCU 12c supports users with lower privileges. In most cases, the master user privilege is sufficient to create repositories.

The master account can directly grant privileges that it has already been granted WITH GRANT OPTION. In some cases, when you attempt to grant SYS object privileges, the RCU might fail with ORA-01031. You can retry and run the `rdsadmin_util.grant_sys_object` stored procedure, as shown in the following example:

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('GV_$SESSION', 'MY_DBA', 'SELECT');
END;
/
```

If you attempt to grant SYS privileges on the object SCHEMA_VERSION_REGISTRY, the operation might fail with ORA-20199: Error in `rdsadmin_util.grant_sys_object`. You can qualify the table SCHEMA_VERSION_REGISTRY\$ and the view SCHEMA_VERSION_REGISTRY with the schema owner name, which is SYSTEM, and retry the operation. Or, you can create a synonym. Log in as the master user and run the following statements:

```
CREATE OR REPLACE VIEW SYSTEM.SCHEMA_VERSION_REGISTRY
AS SELECT * FROM SYSTEM.SCHEMA_VERSION_REGISTRY$;
```

```
CREATE OR REPLACE PUBLIC SYNONYM SCHEMA_VERSION_REGISTRY FOR
SYSTEM.SCHEMA_VERSION_REGISTRY;
CREATE OR REPLACE PUBLIC SYNONYM SCHEMA_VERSION_REGISTRY$ FOR SCHEMA_VERSION_REGISTRY;
```

Enterprise Scheduler Service

When you use the RCU to drop an Enterprise Scheduler Service repository, the RCU might fail with Error: Component drop check failed.

Configuring Oracle Connection Manager on an Amazon EC2 instance

Oracle Connection Manager (CMAN) is a proxy server that forwards connection requests to database servers or other proxy servers. You can use CMAN to configure the following:

Access control

You can create rules that filter out user-specified client requests and accept others.

Session multiplexing

You can funnel multiple client sessions through a network connection to a shared server destination.

Typically, CMAN resides on a host separate from the database server and client hosts. For more information, see [Configuring Oracle Connection Manager](#) in the Oracle Database documentation.

Topics

- [Supported versions and licensing options for CMAN \(p. 1792\)](#)
- [Requirements and limitations for CMAN \(p. 1792\)](#)
- [Configuring CMAN \(p. 1792\)](#)

Supported versions and licensing options for CMAN

CMAN supports the Enterprise Edition of all versions of Oracle Database that Amazon RDS supports. For more information, see [RDS for Oracle releases \(p. 1470\)](#).

You can install Oracle Connection Manager on a separate host from the host where Oracle Database is installed. You don't need a separate license for the host that runs CMAN.

Requirements and limitations for CMAN

To provide a fully managed experience, Amazon RDS restricts access to the operating system. You can't modify database parameters that require operating system access. Thus, Amazon RDS doesn't support features of CMAN that require you to log in to the operating system.

Configuring CMAN

When you configure CMAN, you perform most of the work outside of your RDS for Oracle database.

Topics

- [Step 1: Configure CMAN on an Amazon EC2 instance in the same VPC as the RDS for Oracle instance \(p. 1792\)](#)
- [Step 2: Configure database parameters for CMAN \(p. 1793\)](#)
- [Step 3: Associate your DB instance with the parameter group \(p. 1793\)](#)

Step 1: Configure CMAN on an Amazon EC2 instance in the same VPC as the RDS for Oracle instance

To learn how to set up CMAN, follow the detailed instructions in the blog post [Configuring and using Oracle Connection Manager on Amazon EC2 for Amazon RDS for Oracle](#).

Step 2: Configure database parameters for CMAN

For CMAN features such as Traffic Director Mode and session multiplexing, set REMOTE_LISTENER parameter to the address of CMAN instance in a DB parameter group. Consider the following scenario:

- The CMAN instance resides on a host with IP address 10.0.159.100 and uses port 1521.
- The databases orcla, orclb, and orclc reside on separate RDS for Oracle DB instances.

The following table shows how to set the REMOTE_LISTENER value. The LOCAL_LISTENER value is set automatically by Amazon RDS.

DB instance name	DB instance IP	Local listener value (set automatically)	Remote listener value (set by user)
orcla	10.0.159.200	(address= (protocol=tcp) (host=10.0.159.200) (port=1521))	10.0.159.100:1521
orclb	10.0.159.300	(address= (protocol=tcp) (host=10.0.159.300) (port=1521))	10.0.159.100:1521
orclc	10.0.159.400	(address= (protocol=tcp) (host=10.0.159.400) (port=1521))	10.0.159.100:1521

Step 3: Associate your DB instance with the parameter group

Create or modify your DB instance to use the parameter group that you configured in [Step 2: Configure database parameters for CMAN \(p. 1793\)](#). For more information, see [Associating a DB parameter group with a DB instance \(p. 293\)](#).

Installing a Siebel database on Oracle on Amazon RDS

You can use Amazon RDS to host a Siebel Database on an Oracle DB instance. The Siebel Database is part of the Siebel Customer Relationship Management (CRM) application architecture. For an illustration, see [Generic architecture of Siebel business application](#).

Use the following topic to help set up a Siebel Database on an Oracle DB instance on Amazon RDS. You can also find out how to use Amazon Web Services to support the other components required by the Siebel CRM application architecture.

Note

To install a Siebel Database on Oracle on Amazon RDS, you need to use the master user account. You don't need SYSDBA privilege; master user privilege is sufficient. For more information, see [Master user account privileges \(p. 2087\)](#).

Licensing and versions

To install a Siebel Database on Amazon RDS, you must use your own Oracle Database license, and your own Siebel license. You must have the appropriate Oracle Database license (with Software Update License and Support) for the DB instance class and Oracle Database edition. For more information, see [RDS for Oracle licensing options \(p. 1474\)](#).

Oracle Database Enterprise Edition is the only edition certified by Siebel for this scenario. Amazon RDS supports Siebel CRM version 15.0 or 16.0. Use Oracle Database 12c Release 1 (12.1.0.2.0). For the procedures following, we use Siebel CRM version 15.0 and Oracle Database Release 1 (12.1.0.2) or Oracle Database Release 2 (12.2.0.1). For more information, see [Oracle Database 12c with Amazon RDS \(p. 1473\)](#).

Amazon RDS supports database version upgrades. For more information, see [Upgrading a DB instance engine version \(p. 360\)](#).

Before you begin

Before you begin, you need an Amazon VPC. Because your Amazon RDS DB instance needs to be available only to your Siebel Enterprise Server, and not to the public Internet, your Amazon RDS DB instance is hosted in a private subnet, providing greater security. For information about how to create an Amazon VPC for use with Siebel CRM, see [Creating a VPC for use with an Oracle database \(p. 1767\)](#).

Before you begin, you also need an Oracle DB instance. For information about how to create an Oracle DB instance for use with Siebel CRM, see [Creating an Oracle DB instance \(p. 1772\)](#).

Installing and configuring a Siebel database

After you create your Oracle DB instance, you can install your Siebel Database. You install the database by creating table owner and administrator accounts, installing stored procedures and functions, and then running the Siebel Database Configuration Wizard. For more information, see [Installing the Siebel database on the RDBMS](#).

To run the Siebel Database Configuration Wizard, you need to use the master user account. You don't need SYSDBA privilege; master user privilege is sufficient. For more information, see [Master user account privileges \(p. 2087\)](#).

Using other Amazon RDS features with a Siebel database

After you create your Oracle DB instance, you can use additional Amazon RDS features to help you customize your Siebel Database.

Collecting statistics with the Oracle Statspack option

You can add features to your DB instance through the use of options in DB option groups. When you created your Oracle DB instance, you used the default DB option group. If you want to add features to your database, you can create a new option group for your DB instance.

If you want to collect performance statistics on your Siebel Database, you can add the Oracle Statspack feature. For more information, see [Oracle Statspack \(p. 1739\)](#).

Some option changes are applied immediately, and some option changes are applied during the next maintenance window for the DB instance. For more information, see [Working with option groups \(p. 273\)](#). After you create a customized option group, modify your DB instance to attach it. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Performance tuning with parameters

You manage your DB engine configuration through the use of parameters in a DB parameter group. When you created your Oracle DB instance, you used the default DB parameter group. If you want to customize your database configuration, you can create a new parameter group for your DB instance.

When you change a parameter, depending on the type of the parameter, the changes are applied either immediately or after you manually reboot the DB instance. For more information, see [Working with parameter groups \(p. 289\)](#). After you create a customized parameter group, modify your DB instance to attach it. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

To optimize your Oracle DB instance for Siebel CRM, you can customize certain parameters. The following table shows some recommended parameter settings. For more information about performance tuning Siebel CRM, see [Siebel CRM Performance Tuning Guide](#).

Parameter name	Default value	Guidance for optimal Siebel CRM performance
_always_semi_join	TRUE	OFF
_b_tree_bitmap_index	TRUE	FALSE
_like_with_bind_equality	FALSE	TRUE
_no_or_expansion	FALSE	TRUE
_optimizer_join_elimination_threshold	TRUE	sanity_check
_optimizer_max_parallelizations	2000	100
_optimizer_sortmerge_join_enabled	TRUE	FALSE
_partition_view_enabled	TRUE	FALSE
open_cursors	300	At least 2000.

Creating snapshots

After you create your Siebel Database, you can copy the database by using the snapshot features of Amazon RDS. For more information, see [Creating a DB snapshot \(p. 448\)](#) and [Restoring from a DB snapshot \(p. 452\)](#).

Support for other Siebel CRM components

In addition to your Siebel Database, you can also use Amazon Web Services to support the other components of your Siebel CRM application architecture. You can find more information about the support provided by Amazon AWS for additional Siebel CRM components in the following table.

Siebel CRM component	Amazon AWS Support
Siebel Enterprise (with one or more Siebel Servers)	You can host your Siebel Servers on Amazon Elastic Compute Cloud (Amazon EC2) instances. You can use Amazon EC2 to launch as many or as few virtual servers as you need. Using Amazon EC2, you can scale up or down easily to handle changes in requirements. For more information, see What is Amazon EC2? You can put your servers in the same VPC with your DB instance and use the VPC security group to access the database. For more information, see Working with a DB instance in a VPC (p. 2103) .
Web Servers (with Siebel Web Server Extensions)	You can install multiple Web Servers on multiple EC2 instances. You can then use Elastic Load Balancing to distribute incoming traffic among the instances. For more information, see What is Elastic Load Balancing?
Siebel Gateway Name Server	You can host your Siebel Gateway Name Server on an EC2 instance. You can then put your server in the same VPC with the DB instance and use the VPC security group to access the database. For more information, see Working with a DB instance in a VPC (p. 2103) .

Oracle Database engine release notes

Updates to your Amazon RDS for Oracle DB instances keep them current. If you apply updates, you can be confident that your DB instance is running a version of the database software that has been tested by both Oracle and Amazon. We don't support applying one-off patches to individual RDS for Oracle DB instances.

You can specify any currently supported Oracle Database version when you create a new DB instance. You can specify the major version, such as Oracle Database 19c, and any supported minor version for the specified major version. If no version is specified, Amazon RDS defaults to a supported version, typically the most recent version. If a major version is specified but a minor version is not, Amazon RDS defaults to a recent release of the major version that you have specified. To see a list of supported versions and defaults for newly created DB instances, use the [describe-db-engine-versions](#) AWS CLI command.

For details about the Oracle Database versions that Amazon RDS supports, see the [Amazon RDS for Oracle Release Notes](#).

Amazon RDS for PostgreSQL

Amazon RDS supports DB instances running several versions of PostgreSQL. For a list of available versions, see [Available PostgreSQL database versions \(p. 1805\)](#).

Note

Deprecation of PostgreSQL 9.6 is scheduled for April 26, 2022. For more information, see [Deprecation of PostgreSQL version 10 \(p. 1806\)](#).

You can create DB instances and DB snapshots, point-in-time restores and backups. DB instances running PostgreSQL support Multi-AZ deployments, read replicas, Provisioned IOPS, and can be created inside a virtual private cloud (VPC). You can also use Secure Socket Layer (SSL) to connect to a DB instance running PostgreSQL.

Before creating a DB instance, make sure to complete the steps in [Setting up for Amazon RDS \(p. 148\)](#).

You can use any standard SQL client application to run commands for the instance from your client computer. Such applications include pgAdmin, a popular Open Source administration and development tool for PostgreSQL, or psql, a command line utility that is part of a PostgreSQL installation. To deliver a managed service experience, Amazon RDS doesn't provide host access to DB instances. Also, it restricts access to certain system procedures and tables that require advanced privileges. Amazon RDS supports access to databases on a DB instance using any standard SQL client application. Amazon RDS doesn't allow direct host access to a DB instance by using Telnet or Secure Shell (SSH).

Amazon RDS for PostgreSQL is compliant with many industry standards. For example, you can use Amazon RDS for PostgreSQL databases to build HIPAA-compliant applications and to store healthcare-related information. This includes storage for protected health information (PHI) under a completed Business Associate Agreement (BAA) with AWS. Amazon RDS for PostgreSQL also meets Federal Risk and Authorization Management Program (FedRAMP) security requirements. Amazon RDS for PostgreSQL has received a FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) at the FedRAMP HIGH Baseline within the AWS GovCloud (US) Regions. For more information on supported compliance standards, see [AWS cloud compliance](#).

To import PostgreSQL data into a DB instance, follow the information in the [Importing data into PostgreSQL on Amazon RDS \(p. 1860\)](#) section.

Topics

- [Common management tasks for Amazon RDS for PostgreSQL \(p. 1799\)](#)
- [Working with the database preview environment \(p. 1802\)](#)
- [PostgreSQL version 15 in the database preview environment \(p. 1804\)](#)
- [Available PostgreSQL database versions \(p. 1805\)](#)
- [Supported PostgreSQL extension versions \(p. 1807\)](#)
- [Connecting to a DB instance running the PostgreSQL database engine \(p. 1809\)](#)
- [Securing connections to RDS for PostgreSQL with SSL/TLS \(p. 1816\)](#)
- [Using Kerberos authentication with Amazon RDS for PostgreSQL \(p. 1823\)](#)
- [Using a custom DNS server for outbound network access \(p. 1837\)](#)
- [Upgrading the PostgreSQL DB engine for Amazon RDS \(p. 1839\)](#)
- [Upgrading a PostgreSQL DB snapshot engine version \(p. 1850\)](#)
- [Working with read replicas for Amazon RDS for PostgreSQL \(p. 1852\)](#)
- [Importing data into PostgreSQL on Amazon RDS \(p. 1860\)](#)
- [Exporting data from an RDS for PostgreSQL DB instance to Amazon S3 \(p. 1883\)](#)
- [Invoking an AWS Lambda function from an RDS for PostgreSQL DB instance \(p. 1895\)](#)
- [Working with PostgreSQL features supported by Amazon RDS for PostgreSQL \(p. 1905\)](#)

- [Common DBA tasks for Amazon RDS for PostgreSQL \(p. 1915\)](#)
- [Using PostgreSQL extensions with Amazon RDS for PostgreSQL \(p. 1945\)](#)
- [Working with the supported foreign data wrappers for Amazon RDS for PostgreSQL \(p. 1987\)](#)

Common management tasks for Amazon RDS for PostgreSQL

The following are the common management tasks you perform with an Amazon RDS for PostgreSQL DB instance, with links to relevant documentation for each task.

Task area	Relevant documentation
Setting up Amazon RDS for first-time use Before you can create your DB instance, make sure to complete a few prerequisites. For example, DB instances are created by default with a firewall that prevents access to it. So you need to create a security group with the correct IP addresses and network configuration to access the DB instance.	Setting up for Amazon RDS (p. 148)
Understanding Amazon RDS DB instances If you are creating a DB instance for production purposes, you should understand how instance classes, storage types, and Provisioned IOPS work in Amazon RDS.	DB instance classes (p. 10) Amazon RDS storage types (p. 64) Provisioned IOPS SSD storage (p. 66)
Finding available PostgreSQL versions Amazon RDS supports several versions of PostgreSQL.	Available PostgreSQL database versions (p. 1805)
Setting up high availability and failover support A production DB instance should use Multi-AZ deployments. Multi-AZ deployments provide increased availability, data durability, and fault tolerance for DB instances.	Multi-AZ deployments for high availability (p. 121)
Understanding the Amazon Virtual Private Cloud (VPC) network If your AWS account has a default VPC, then your DB instance is automatically created inside the default VPC. In some cases, your account might not have a default VPC, and you might want the DB instance in a VPC. In these cases, create the VPC and subnet groups before you create the DB instance.	Working with a DB instance in a VPC (p. 2103)
Importing data into Amazon RDS PostgreSQL You can use several different tools to import data into your PostgreSQL DB instance on Amazon RDS.	Importing data into PostgreSQL on Amazon RDS (p. 1860)
Setting up read-only read replicas (primary and standbys) RDS for PostgreSQL supports read replicas in both the same AWS Region and in a different AWS Region from the primary instance.	Working with read replicas (p. 370)

Task area	Relevant documentation
	Working with read replicas for Amazon RDS for PostgreSQL (p. 1852) Creating a read replica in a different AWS Region (p. 383)
Understanding security groups <p>By default, DB instances are created with a firewall that prevents access to them. To provide access through that firewall, you edit the inbound rules for the VPC security group associated with the VPC hosting the DB instance.</p>	Controlling access with security groups (p. 2085)
Setting up parameter groups and features <p>To change the default parameters for your DB instance, create a custom DB parameter group and change settings to that. If you do this before creating your DB instance, you can choose your custom DB parameter group when you create the instance.</p>	Working with parameter groups (p. 289)
Connecting to your PostgreSQL DB instance <p>After creating a security group and associating it to a DB instance, you can connect to the DB instance using any standard SQL client application such as psql or pgAdmin.</p>	Connecting to a DB instance running the PostgreSQL database engine (p. 1809) Using SSL with a PostgreSQL DB instance (p. 1816)
Backing up and restoring your DB instance <p>You can configure your DB instance to take automated backups, or take manual snapshots, and then restore instances from the backups or snapshots.</p>	Backing up and restoring an Amazon RDS DB instance (p. 426)
Monitoring the activity and performance of your DB instance <p>You can monitor a PostgreSQL DB instance by using CloudWatch Amazon RDS metrics, events, and enhanced monitoring.</p>	Viewing metrics in the Amazon RDS console (p. 525) Viewing Amazon RDS events (p. 647)
Upgrading the PostgreSQL database version <p>You can do both major and minor version upgrades for your PostgreSQL DB instance.</p>	Upgrading the PostgreSQL DB engine for Amazon RDS (p. 1839) Choosing a major version upgrade for PostgreSQL (p. 1841)
Working with log files <p>You can access the log files for your PostgreSQL DB instance.</p>	RDS for PostgreSQL database log files (p. 716)
Understanding the best practices for PostgreSQL DB instances <p>Find some of the best practices for working with PostgreSQL on Amazon RDS.</p>	Best practices for working with PostgreSQL (p. 224)

Following is a list of other sections in this guide that can help you understand and use important features of RDS for PostgreSQL:

- [Understanding PostgreSQL roles and permissions \(p. 1915\)](#)
- [Controlling user access to the PostgreSQL database \(p. 1917\)](#)
- [Working with parameters on your RDS for PostgreSQL DB instance \(p. 1934\)](#)
- [Understanding logging mechanisms supported by RDS for PostgreSQL \(p. 1933\)](#)
- [Working with the PostgreSQL autovacuum on Amazon RDS for PostgreSQL \(p. 1924\)](#)
- [Using a custom DNS server for outbound network access \(p. 1837\)](#)

Working with the database preview environment

The PostgreSQL community continuously releases new PostgreSQL version and extensions, including beta versions. This gives PostgreSQL users the opportunity to try out a new PostgreSQL version early. To learn more about the PostgreSQL community beta release process, see [Beta Information](#) in the PostgreSQL documentation. Similarly, Amazon RDS makes certain PostgreSQL beta versions available as Preview releases. This allows you to create DB instances using the Preview version and test out its features in the Database Preview Environment.

RDS for PostgreSQL DB instances in the Database Preview Environment are functionally similar to other RDS for PostgreSQL instances. However, you can't use a Preview version for production.

Keep in mind the following important limitations:

- All DB instances are deleted 60 days after you create them, along with any backups and snapshots.
- You can only create a DB instance in a virtual private cloud (VPC) based on the Amazon VPC service.
- You can only use General Purpose SSD and Provisioned IOPS SSD storage.
- You can't get help from AWS Support with DB instances. Instead, you can post your questions to the AWS-managed Q&A community, [AWS re:Post](#).
- You can't copy a snapshot of a DB instance to a production environment.

The following options are supported by the Preview.

- You can create DB instances using M6i, R6i, M6g, M5, T3, R6g, and R5 instance types only. For more information about RDS instance classes, see [DB instance classes \(p. 10\)](#).
- You can use both single-AZ and multi-AZ deployments.
- You can use standard PostgreSQL dump and load functions to export databases from or import databases to the Database Preview Environment.

Features not supported in the preview environment

The following features aren't available in the preview environment:

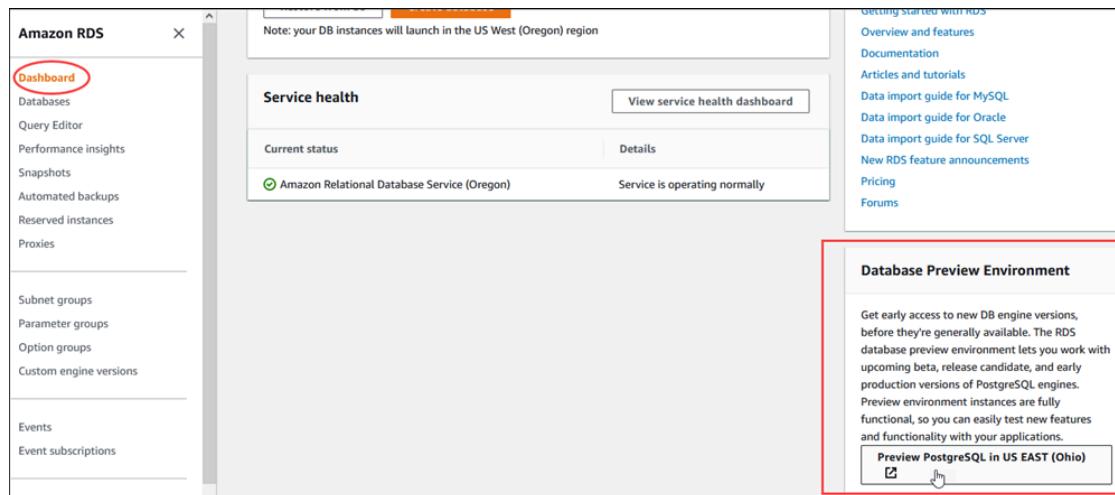
- Cross-Region snapshot copy
- Cross-Region read replicas

Creating a new DB instance in the preview environment

Use the following procedure to create a DB instance in the preview environment.

To create a DB instance in the preview environment

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose **Dashboard** from the navigation pane.
3. In the Dashboard page, locate the **Database Preview Environment** section on the Dashboard page, as shown in the following image.



You can navigate directly to the [Database preview environment](#). Before you can proceed, you must acknowledge and accept the limitations.

The Amazon RDS Database Preview Environment is not covered by the Amazon RDS service level agreement (SLA), published at <http://aws.amazon.com/rds-sla/>.

Do not use the Amazon RDS Database Preview Environment for production purposes. You should only use this environment for development and testing.

Certain use cases might fail in this environment - for example, upgrading from a previous version is not supported.

I acknowledge this limited service agreement for the Amazon RDS Database Preview Environment and that I should only use this environment for development and testing.

[Cancel](#) [Accept](#)

4. To create the RDS for PostgreSQL DB instance, follow the same process as that for creating any Amazon RDS DB instance. For more information, see the [Console \(p. 233\)](#) procedure in [Creating a DB instance \(p. 233\)](#).

To create an instance in the Database Preview Environment using the RDS API or the AWS CLI, use the following endpoint.

rds-preview.us-east-2.amazonaws.com

PostgreSQL version 15 in the database preview environment

PostgreSQL version 15 is now available in the Amazon RDS Database Preview Environment. PostgreSQL version 15 contains several improvements that are described in the following PostgreSQL documentation:

- [PostgreSQL 15](#)
- [PostgreSQL 15 Beta 3 Released!](#)

For information on the Database Preview Environment, see [the section called “The database preview environment” \(p. 1802\)](#). To access the Preview Environment from the console, select <https://console.aws.amazon.com/rds-preview/>.

Available PostgreSQL database versions

Amazon RDS supports DB instances running several editions of PostgreSQL. You can specify any currently available PostgreSQL version when creating a new DB instance. You can specify the major version (such as PostgreSQL 14), and any available minor version for the specified major version. If no version is specified, Amazon RDS defaults to an available version, typically the most recent version. If a major version is specified but a minor version is not, Amazon RDS defaults to a recent release of the major version you have specified.

To see a list of available versions, as well as defaults for newly created DB instances, use the [describe-db-engine-versions](#) AWS CLI command. For example, to display the default PostgreSQL engine version, use the following command:

```
aws rds describe-db-engine-versions --default-only --engine postgres
```

For details about the PostgreSQL versions that are supported on Amazon RDS, see the [Amazon RDS for PostgreSQL Release Notes](#).

Deprecation of PostgreSQL version 10

On April 17, 2023, Amazon RDS plans to deprecate PostgreSQL 10 using the following schedule. We recommend that you take action and upgrade your PostgreSQL databases running on major version 10 to a later version, such as PostgreSQL version 14. To upgrade your RDS for PostgreSQL major version 10 DB instance from a PostgreSQL version older than 10.19, we recommend that you first upgrade to version 10.19 and then upgrade to version 14. For more information, see [Upgrading the PostgreSQL DB engine for Amazon RDS \(p. 1839\)](#).

Action or recommendation	Dates
The PostgreSQL community plans to deprecate PostgreSQL 10 and won't provide any security patches after this date.	November 10, 2022
Start upgrading RDS for PostgreSQL 10 DB instances to a later major version, such as PostgreSQL 14. Although you can continue to restore PostgreSQL 10 snapshots and create read replicas with version 10, be aware of the other critical dates in this deprecation schedule and their impact.	Now – February 14, 2023
After this date, you can't create new Amazon RDS instances with PostgreSQL major version 10 from either the AWS Management Console or the AWS CLI.	February 14, 2023
After this date, Amazon RDS automatically upgrades PostgreSQL 10 instances to version 14. If you restore a PostgreSQL 10 database snapshot, Amazon RDS automatically upgrades the restored database to PostgreSQL 14.	April 17, 2023

For more information about RDS for PostgreSQL version 10 deprecation, see [\[Announcement\]: RDS for PostgreSQL 10 deprecation](#) in AWS re:Post.

Deprecation of PostgreSQL version 9.6

On March 31, 2022, Amazon RDS plans to deprecate PostgreSQL 9.6 using the following schedule. This extends the previously announced date of January 18, 2022 to April 26, 2022. You should upgrade all your PostgreSQL 9.6 DB instances to PostgreSQL 12 or higher as soon as possible. We recommend that you first upgrade to minor version 9.6.20 or higher and then upgrade directly to PostgreSQL 12 rather than upgrading to an intermediate major version. For more information, see [Upgrading the PostgreSQL DB engine for Amazon RDS \(p. 1839\)](#).

Action or recommendation	Dates
The PostgreSQL community discontinued support for PostgreSQL 9.6, and will no longer provide bug fixes or security patches for this version.	November 11, 2021
Start upgrading RDS for PostgreSQL 9.6 DB instances to PostgreSQL 12 or higher as soon as possible. Although you can continue to restore PostgreSQL 9.6 snapshots and create read replicas with version 9.6, be aware of the other critical dates in this deprecation schedule and their impact.	Now – March 31, 2022
After this date, you can't create new Amazon RDS instances with PostgreSQL major version 9.6 from either the AWS Management Console or the AWS CLI.	March 31, 2022
After this date, Amazon RDS automatically upgrades PostgreSQL 9.6 instances to version 12. If you restore a PostgreSQL 9.6 database snapshot, Amazon RDS automatically upgrades the restored database to PostgreSQL 12.	April 26, 2022

Deprecated versions for Amazon RDS for PostgreSQL

RDS for PostgreSQL 9.5 is deprecated as of March, 2021. For more information about RDS for PostgreSQL 9.5 deprecation, see [Upgrading from Amazon RDS for PostgreSQL version 9.5](#).

To learn more about deprecation policy for RDS for PostgreSQL, see [Amazon RDS FAQs](#). For more information about PostgreSQL versions, see [Versioning Policy](#) in the PostgreSQL documentation.

Supported PostgreSQL extension versions

RDS for PostgreSQL supports many PostgreSQL extensions. The PostgreSQL community sometimes refers to these as modules. Extensions expand on the functionality provided by the PostgreSQL engine. You can find a list of extensions supported by Amazon RDS in the default DB parameter group for that PostgreSQL version. You can also see the current extensions list using `psql` by showing the `rds.extensions` parameter as in the following example.

```
SHOW rds.extensions;
```

Note

Parameters added in a minor version release might display inaccurately when using the `rds.extensions` parameter in `psql`.

As of RDS for PostgreSQL 13, certain extensions can be installed by database users other than the `rds_superuser`. These are known as *trusted extensions*. To learn more, see [PostgreSQL trusted extensions \(p. 1808\)](#).

Certain versions of RDS for PostgreSQL support the `rds.allowed_extensions` parameter. This parameter lets an `rds_superuser` limit the extensions that can be installed in the RDS for PostgreSQL DB instance. For more information, see [Restricting installation of PostgreSQL extensions \(p. 1807\)](#).

For lists of PostgreSQL extensions and versions that are supported by each available RDS for PostgreSQL version, see [PostgreSQL extensions supported on Amazon RDS](#) in *Amazon RDS for PostgreSQL Release Notes*.

Restricting installation of PostgreSQL extensions

You can restrict which extensions can be installed on a PostgreSQL DB instance. To do so, set the `rds.allowed_extensions` parameter to a string of comma-separated extension names. Only these extensions can then be installed in the PostgreSQL DB instance.

The default string for the `rds.allowed_extensions` parameter is `*`, which means that any extension available for the engine version can be installed. Changing the `rds.allowed_extensions` parameter does not require a database restart because it's a dynamic parameter.

The PostgreSQL DB instance engine must be one of the following versions for you to use the `rds.allowed_extensions` parameter:

- PostgreSQL 14.1 or a higher minor version
- PostgreSQL 13.2 or a higher minor version
- PostgreSQL 12.6 or a higher minor version

To see which extension installations are allowed, use the following `psql` command.

```
postgres=> SHOW rds.allowed_extensions;
rds.allowed_extensions
-----
*
```

If an extension was installed prior to it being left out of the list in the `rds.allowed_extensions` parameter, the extension can still be used normally, and commands such as `ALTER EXTENSION` and `DROP EXTENSION` will continue to work. However, after an extension is restricted, `CREATE EXTENSION` commands for the restricted extension will fail.

Installation of extension dependencies with `CREATE EXTENSION CASCADE` are also restricted. The extension and its dependencies must be specified in `rds.allowed_extensions`. If an extension dependency installation fails, the entire `CREATE EXTENSION CASCADE` statement will fail.

If an extension is not included with the `rds.allowed_extensions` parameter, you will see an error such as the following if you try to install it.

```
ERROR: permission denied to create extension "extension-name"  
HINT: This extension is not specified in "rds.allowed_extensions".
```

PostgreSQL trusted extensions

To install most PostgreSQL extensions requires `rds_superuser` privileges. PostgreSQL 13 introduced trusted extensions, which reduce the need to grant `rds_superuser` privileges to regular users. With this feature, users can install many extensions if they have the `CREATE` privilege on the current database instead of requiring the `rds_superuser` role. For more information, see the SQL [CREATE EXTENSION](#) command in the PostgreSQL documentation.

The following lists the extensions that can be installed by a user who has the `CREATE` privilege on the current database and do not require the `rds_superuser` role:

- [bool_plperl](#)
- [btree_gin](#)
- [btree_gist](#)
- [citext](#)
- [cube](#)
- [dict_int](#)
- [fuzzystrmatch](#)
- [hstore](#)
- [intarray](#)
- [isn](#)
- [jsonb_plperl](#)
- [ltree](#)
- [pg_trgm](#)
- [pgcrypto](#)
- [plperl](#)
- [plpgsql](#)
- [pltcl](#)
- [tablefunc](#)
- [tsm_system_rows](#)
- [tsm_system_time](#)
- [unaccent](#)
- [uuid-ossp](#)

For lists of PostgreSQL extensions and versions that are supported by each available RDS for PostgreSQL version, see [PostgreSQL extensions supported on Amazon RDS](#) in *Amazon RDS for PostgreSQL Release Notes*.

Connecting to a DB instance running the PostgreSQL database engine

After Amazon RDS provisions your DB instance, you can use any standard SQL client application to connect to the instance. Before you can connect, the DB instance must be available and accessible. Whether you can connect to the instance from outside the VPC depends on how you created the Amazon RDS DB instance:

- If you created your DB instance as *public*, devices and Amazon EC2 instances outside the VPC can connect to your database.
- If you created your DB instance as *private*, only Amazon EC2 instances and devices inside the Amazon VPC can connect to your database.

To check whether your DB instance is public or private, use the AWS Management Console to view the **Connectivity & security** tab for your instance. Under **Security**, you can find the "Publicly accessible" value, with No for private, Yes for public.

To learn more about different Amazon RDS and Amazon VPC configurations and how they affect accessibility, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

If the DB instance is available and accessible, you can connect by providing the following information to the SQL client application:

- The DB instance endpoint, which serves as the host name (DNS name) for the instance.
- The port on which the DB instance is listening. For PostgreSQL, the default port is 5432.
- The user name and password for the DB instance. The default 'master username' for PostgreSQL is `postgres`.
- The name and password of the database (DB name).

You can obtain these details by using the AWS Management Console, the AWS CLI [describe-db-instances](#) command, or the Amazon RDS API [DescribeDBInstances](#) operation.

To find the endpoint, port number, and DB name using the AWS Management Console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Open the RDS console and then choose **Databases** to display a list of your DB instances.
3. Choose the PostgreSQL DB instance name to display its details.
4. On the **Connectivity & security** tab, copy the endpoint. Also, note the port number. You need both the endpoint and the port number to connect to the DB instance.

The screenshot shows the 'Summary' tab for a database named 'database-1'. It displays the DB identifier as 'database-1' and the role as 'Instance'. Below the summary, there are three tabs: 'Connectivity & security' (which is highlighted in orange), 'Monitoring', and 'Logs & events'. The 'Connectivity & security' tab is expanded, showing the 'Endpoint & port' section. The 'Endpoint' field contains 'database-1.' followed by a blurred address, and 'us-west-1.rds.amazonaws.com'. The 'Port' field is listed as '5432'. Both the 'Endpoint' and 'Port' fields are circled in red.

5. On the **Configuration** tab, note the DB name. If you created a database when you created the RDS for PostgreSQL instance, you see the name listed under DB name. If you didn't create a database, the DB name displays a dash (-).

Connectivity & security	Monitoring	Logs & events	Configuration
Instance			
Configuration	Instance class	Storage	
DB instance ID database-1	Instance class db.m5.large	Encryption Enabled	
Engine version 13.4	vCPU 2	AWS KMS key aws/rds ↗	
DB name labdb	RAM 8 GB	Storage type General Purpose	

Following are two ways to connect to a PostgreSQL DB instance. The first example uses pgAdmin, a popular open-source administration and development tool for PostgreSQL. The second example uses psql, a command line utility that is part of a PostgreSQL installation.

Topics

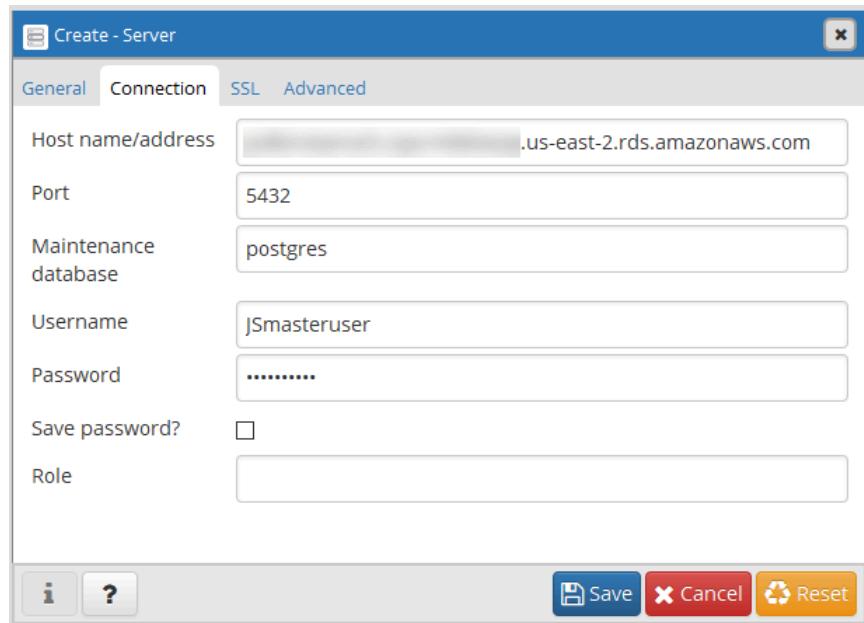
- [Using pgAdmin to connect to a RDS for PostgreSQL DB instance \(p. 1811\)](#)
- [Using psql to connect to your RDS for PostgreSQL DB instance \(p. 1813\)](#)
- [Connecting with the AWS JDBC Driver for PostgreSQL \(p. 1813\)](#)
- [Troubleshooting connections to your RDS for PostgreSQL instance \(p. 1814\)](#)

Using pgAdmin to connect to a RDS for PostgreSQL DB instance

You can use the open-source tool pgAdmin to connect to your RDS for PostgreSQL DB instance. You can download and install pgAdmin from <http://www.pgadmin.org/> without having a local instance of PostgreSQL on your client computer.

To connect to your RDS for PostgreSQL DB instance using pgAdmin

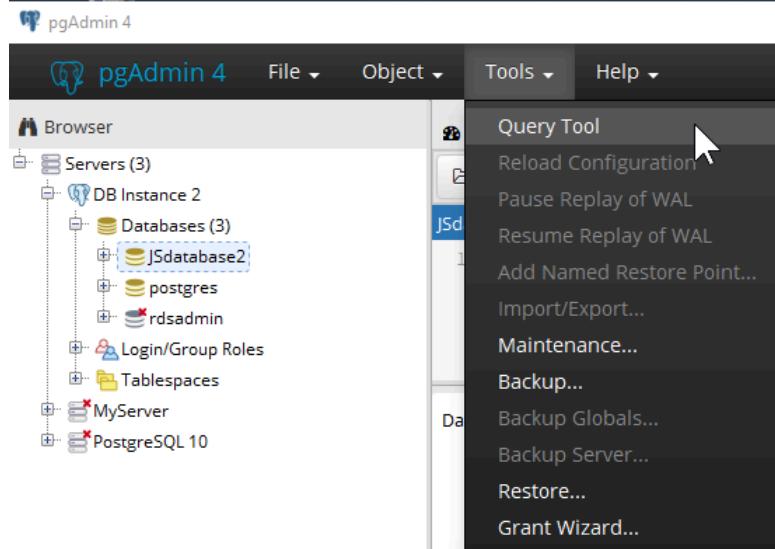
1. Launch the pgAdmin application on your client computer.
2. On the **Dashboard** tab, choose **Add New Server**.
3. In the **Create - Server** dialog box, type a name on the **General** tab to identify the server in pgAdmin.
4. On the **Connection** tab, type the following information from your DB instance:
 - For **Host**, type the endpoint, for example mypostgresql.c6c8dntfzzhgv0.us-east-2.rds.amazonaws.com.
 - For **Port**, type the assigned port.
 - For **Username**, type the user name that you entered when you created the DB instance (if you changed the 'master username' from the default, postgres).
 - For **Password**, type the password that you entered when you created the DB instance.



5. Choose **Save**.

If you have any problems connecting, see [Troubleshooting connections to your RDS for PostgreSQL instance \(p. 1814\)](#).

6. To access a database in the pgAdmin browser, expand **Servers**, the DB instance, and **Databases**. Choose the DB instance's database name.



7. To open a panel where you can enter SQL commands, choose **Tools**, **Query Tool**.

Using psql to connect to your RDS for PostgreSQL DB instance

You can use a local instance of the psql command line utility to connect to a RDS for PostgreSQL DB instance. You need either PostgreSQL or the psql client installed on your client computer.

To connect to your RDS for PostgreSQL DB instance using psql, you need to provide host (DNS) information, access credentials, and the name of the database.

Use one of the following formats to connect to your RDS for PostgreSQL DB instance. When you connect, you're prompted for a password. For batch jobs or scripts, use the `--no-password` option. This option is set for the entire session.

Note

A connection attempt with `--no-password` fails when the server requires password authentication and a password is not available from other sources. For more information, see the [psql documentation](#).

If this is the first time you are connecting to this DB instance, or if you didn't yet create a database for this RDS for PostgreSQL instance, you can connect to the `postgres` database using the 'master username' and password.

For Unix, use the following format.

```
psql \
--host=<DB instance endpoint> \
--port=<port> \
--username=<master username> \
--password \
--dbname=<database name>
```

For Windows, use the following format.

```
psql ^
--host=<DB instance endpoint> ^
--port=<port> ^
--username=<master username> ^
--password ^
--dbname=<database name>
```

For example, the following command connects to a database called `mypgdb` on a PostgreSQL DB instance called `mypostgresql` using fictitious credentials.

```
psql --host=mypostgresql.c6c8mwvfdgv0.us-west-2.rds.amazonaws.com --port=5432 --
username=awsuser --password --dbname=mypgdb
```

Connecting with the AWS JDBC Driver for PostgreSQL

The AWS JDBC Driver for PostgreSQL is a client wrapper designed for use with RDS for PostgreSQL. The AWS JDBC Driver for PostgreSQL extends the functionality of the community pgJDBC driver by enabling AWS features such as authentication. For more information about the AWS JDBC Driver for PostgreSQL and complete instructions for using it, see the [AWS JDBC Driver for PostgreSQL GitHub repository](#).

The AWS JDBC Driver for PostgreSQL supports AWS Identity and Access Management (IAM) database authentication and AWS Secrets Manager. For more information on using these authentication

mechanisms with the driver, see [AWS IAM Authentication Plugin](#) and [AWS Secrets Manager Plugin](#) in the AWS JDBC Driver for PostgreSQL GitHub repository.

For more information about IAM database authentication, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#). For more information about Secrets Manager, see the [AWS Secrets Manager User Guide](#).

Troubleshooting connections to your RDS for PostgreSQL instance

Topics

- [Error – FATAL: database *name* does not exist \(p. 1814\)](#)
- [Error – Could not connect to server: Connection timed out \(p. 1814\)](#)
- [Errors with security group access rules \(p. 1814\)](#)

Error – FATAL: database *name* does not exist

If when trying to connect you receive an error like FATAL: database *name* does not exist, try using the default database name **postgres** for the --dbname option.

Error – Could not connect to server: Connection timed out

If you can't connect to the DB instance, the most common error is Could not connect to server: Connection timed out. If you receive this error, check the following:

- Check that the host name used is the DB instance endpoint and that the port number used is correct.
- Make sure that the DB instance's public accessibility is set to Yes to allow external connections. To modify the **Public access** setting, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- Check that the security group assigned to the DB instance has rules to allow access through any firewall your connection might go through. For example, if the DB instance was created using the default port of 5432, your company might have firewall rules blocking connections to that port from external company devices.

To fix this, modify the DB instance to use a different port. Also, make sure that the security group applied to the DB instance allows connections to the new port. To modify the **Database port** setting, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

- See also [Errors with security group access rules \(p. 1814\)](#).

Errors with security group access rules

By far the most common connection problem is with the security group's access rules assigned to the DB instance. If you used the default security group when you created the DB instance, the security group likely didn't have access rules that allow you to access the instance.

For the connection to work, the security group you assigned to the DB instance at its creation must allow access to the DB instance. For example, if the DB instance was created in a VPC, it must have a VPC security group that authorizes connections. Check if the DB instance was created using a security group that doesn't authorize connections from the device or Amazon EC2 instance where the application is running.

You can add or edit an inbound rule in the security group. For **Source**, choosing **My IP** allows access to the DB instance from the IP address detected in your browser. For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

Alternatively, if the DB instance was created outside of a VPC, it must have a database security group that authorizes those connections.

For more information about Amazon RDS security groups, see [Controlling access with security groups \(p. 2085\)](#).

Securing connections to RDS for PostgreSQL with SSL/TLS

RDS for PostgreSQL supports Secure Socket Layer (SSL) encryption for PostgreSQL DB instances. Using SSL, you can encrypt a PostgreSQL connection between your applications and your PostgreSQL DB instances. You can also force all connections to your PostgreSQL DB instance to use SSL. RDS for PostgreSQL also supports Transport Layer Security (TLS), the successor protocol to SSL.

To learn more about Amazon RDS and data protection, including encrypting connections using SSL/TLS, see [Data protection in Amazon RDS \(p. 1999\)](#).

Topics

- [Using SSL with a PostgreSQL DB instance \(p. 1816\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1819\)](#)

Using SSL with a PostgreSQL DB instance

Amazon RDS supports Secure Socket Layer (SSL) encryption for PostgreSQL DB instances. Using SSL, you can encrypt a PostgreSQL connection between your applications and your PostgreSQL DB instances. By default, RDS for PostgreSQL uses and expects all clients to connect using SSL/TLS, but you can also require it. RDS for PostgreSQL supports Transport Layer Security (TLS) versions 1.1 and 1.2.

For general information about SSL support and PostgreSQL databases, see [SSL support](#) in the PostgreSQL documentation. For information about using an SSL connection over JDBC, see [Configuring the client](#) in the PostgreSQL documentation.

SSL support is available in all AWS Regions for PostgreSQL. Amazon RDS creates an SSL certificate for your PostgreSQL DB instance when the instance is created. If you enable SSL certificate verification, then the SSL certificate includes the DB instance endpoint as the Common Name (CN) for the SSL certificate to guard against spoofing attacks.

Topics

- [Connecting to a PostgreSQL DB instance over SSL \(p. 1816\)](#)
- [Requiring an SSL connection to a PostgreSQL DB instance \(p. 1817\)](#)
- [Determining the SSL connection status \(p. 1817\)](#)
- [SSL cipher suites in RDS for PostgreSQL \(p. 1819\)](#)

Connecting to a PostgreSQL DB instance over SSL

To connect to a PostgreSQL DB instance over SSL

1. Download the certificate.

For information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

2. Import the certificate into your operating system.

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

3. Connect to your PostgreSQL DB instance over SSL.

When you connect using SSL, your client can choose whether to verify the certificate chain. If your connection parameters specify `sslmode=verify-ca` or `sslmode=verify-full`, then your client requires the RDS CA certificates to be in their trust store or referenced in the connection URL. This requirement is to verify the certificate chain that signs your database certificate.

When a client, such as `psql` or JDBC, is configured with SSL support, the client first tries to connect to the database with SSL by default. If the client can't connect with SSL, it reverts to connecting without SSL. The default `sslmode` mode used is different between libpq-based clients (such as `psql`) and JDBC. The libpq-based clients default to `prefer`, and JDBC clients default to `verify-full`.

Use the `sslrootcert` parameter to reference the certificate, for example `sslrootcert=rds-ssl-ca-cert.pem`.

The following is an example of using `psql` to connect to a PostgreSQL DB instance using SSL with certificate verification.

```
$ psql -h db-name.55555555555.ap-southeast-1.rds.amazonaws.com  
-p 5432 dbname=testDB user=testuser sslrootcert=rds-ca-2019-root.pem sslmode=verify-full
```

Requiring an SSL connection to a PostgreSQL DB instance

You can require that connections to your PostgreSQL DB instance use SSL by using the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to 0 (off). You can set the `rds.force_ssl` parameter to 1 (on) to require SSL for connections to your DB instance.

To change the value of this parameter, you need to create a custom DB parameter group. You then change the value for `rds.force_ssl` in your custom DB parameter group to 1 to turn on this feature. If you prepare the custom DB parameter group before creating your RDS for PostgreSQL DB instance you can choose it (instead of a default parameter group) during the creation process. If you do this after your RDS for PostgreSQL DB instance is already running, you need to reboot the instance so that your instance uses the custom parameter group. For more information, see [Working with parameter groups \(p. 289\)](#).

When the `rds.force_ssl` feature is active on your DB instance, connection attempts that aren't using SSL are rejected with the following message:

```
$ psql -h db-name.55555555555.ap-southeast-1.rds.amazonaws.com -p 5432 dbname=testDB  
user=testuser  
psql: error: FATAL: no pg_hba.conf entry for host "w.x.y.z", user "testuser", database  
"testDB", SSL off
```

Determining the SSL connection status

The encrypted status of your connection is shown in the logon banner when you connect to the DB instance:

```
Password for user master:  
psql (10.3)  
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)  
Type "help" for help.  
postgres=>
```

You can also load the `sslinfo` extension and then call the `ssl_is_used()` function to determine if SSL is being used. The function returns `t` if the connection is using SSL, otherwise it returns `f`.

```
postgres=> CREATE EXTENSION sslinfo;
CREATE EXTENSION
postgres=> SELECT ssl_is_used();
ssl_is_used
-----
t
(1 row)
```

For more detailed information, you can use the following query to get information from pg_settings:

Parameter name	value	
short_desc		
ssl	on	Enables SSL connections.
ssl_ca_file	/rdsdbdata/rds-metadata/ca-cert.pem	Location of the SSL certificate authority file.
ssl_cert_file	/rdsdbdata/rds-metadata/server-cert.pem	Location of the SSL server certificate file.
ssl_ciphers	HIGH:!aNULL:!3DES	Sets the list of allowed SSL ciphers.
ssl_crl_file		Location of the SSL certificate revocation list file.
ssl_dh_params_file		Location of the SSL DH parameters file.
ssl_ecdh_curve	prime256v1	Sets the curve to use for ECDH.
ssl_key_file	/rdsdbdata/rds-metadata/server-key.pem	Location of the SSL server private key file.
ssl_library	OpenSSL	Name of the SSL library.
ssl_max_protocol_version		Sets the maximum SSL/TLS protocol version to use.
ssl_min_protocol_version	TLSv1.2	Sets the minimum SSL/TLS protocol version to use.
ssl_passphrase_command		Command to obtain passphrases for SSL.
ssl_passphrase_command_supports_reload	off	Also use ssl_passphrase_command during server reload.
ssl_prefer_server_ciphers	on	Give priority to server ciphersuite order.

(14 rows)

You can also collect all the information about your RDS for PostgreSQL DB instance's SSL usage by process, client, and application by using the following query:

```
SELECT datname as "Database name", username as "User name", ssl, client_addr,
application_name, backend_type
  FROM pg_stat_ssl
  JOIN pg_stat_activity
    ON pg_stat_ssl.pid = pg_stat_activity.pid
   ORDER BY ssl;
Database name | User name | ssl | client_addr | application_name | backend_type
-----+-----+-----+-----+
launcher      |          | f  |           |                  | autovacuum
                | rdsadmin | f  |           |                  | logical
replication launcher
```

writer		f					background
			f				checkpointer
rdsadmin	rdsadmin		f				walwriter
rdsadmin	rdsadmin	t		127.0.0.1			client backend
postgres	postgres	t		127.0.0.1	PostgreSQL JDBC Driver		client backend
(8 rows)				204.246.162.36	psql		client backend

To identify the cipher used for your SSL connection, you can query as follows:

```
postgres=> SELECT ssl_cipher();
ssl_cipher
-----
DHE-RSA-AES256-SHA
(1 row)
```

To learn more about the `sslmode` option, see [Database connection control functions](#) in the *PostgreSQL documentation*.

SSL cipher suites in RDS for PostgreSQL

The PostgreSQL configuration parameter `ssl_ciphers` specifies the categories of cipher suites that are allowed for SSL connections. The following table lists the default cipher suites used in RDS for PostgreSQL.

PostgreSQL engine version	Cipher suites
14	HIGH:!aNULL:!3DES
13	HIGH:!aNULL:!3DES
12	HIGH:!aNULL:!3DES
11.4 and higher minor versions	HIGH:MEDIUM:+3DES:!aNULL:!RC4
11.1, 11.2	HIGH:MEDIUM:+3DES:!aNULL
10.9 and higher minor versions	HIGH:MEDIUM:+3DES:!aNULL:!RC4
10.7 and lower minor versions	HIGH:MEDIUM:+3DES:!aNULL

Updating applications to use new SSL/TLS certificates

Certificates used for Secure Socket Layer or Transport Layer Security (SSL/TLS) typically have a set lifetime. When service providers update their Certificate Authority (CA) certificates, clients must update their applications to use the new certificates. Following, you can find information about how to determine if your client applications use SSL/TLS to connect to your Amazon RDS for PostgreSQL DB instance. You also find information about how to check if those applications verify the server certificate when they connect.

Note

A client application that's configured to verify the server certificate before SSL/TLS connection must have a valid CA certificate in the client's trust store. Update the client trust store when necessary for new certificates.

After you update your CA certificates in the client application trust stores, you can rotate the certificates on your DB instances. We strongly recommend testing these procedures in a nonproduction environment before implementing them in your production environments.

For more information about certificate rotation, see [Rotating your SSL/TLS certificate \(p. 2007\)](#). For more information about downloading certificates, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). For information about using SSL/TLS with PostgreSQL DB instances, see [Using SSL with a PostgreSQL DB instance \(p. 1816\)](#).

Topics

- [Determining whether applications are connecting to PostgreSQL DB instances using SSL \(p. 1820\)](#)
- [Determining whether a client requires certificate verification in order to connect \(p. 1820\)](#)
- [Updating your application trust store \(p. 1821\)](#)
- [Using SSL/TLS connections for different types of applications \(p. 1821\)](#)

Determining whether applications are connecting to PostgreSQL DB instances using SSL

Check the DB instance configuration for the value of the `rds.force_ssl` parameter. By default, the `rds.force_ssl` parameter is set to 0 (off). If the `rds.force_ssl` parameter is set to 1 (on), clients are required to use SSL/TLS for connections. For more information about parameter groups, see [Working with parameter groups \(p. 289\)](#).

If you are using RDS PostgreSQL version 9.5 or later major version and `rds.force_ssl` is not set to 1 (on), query the `pg_stat_ssl` view to check connections using SSL. For example, the following query returns only SSL connections and information about the clients using SSL.

```
SELECT datname, username, ssl, client_addr
  FROM pg_stat_ssl INNER JOIN pg_stat_activity ON pg_stat_ssl.pid = pg_stat_activity.pid
 WHERE ssl is true and username<>'rdsadmin';
```

Only rows using SSL/TLS connections are displayed with information about the connection. The following is sample output.

```
datname | username | ssl | client_addr
-----+-----+-----+
benchdb | pgadmin | t   | 53.95.6.13
postgres | pgadmin | t   | 53.95.6.13
(2 rows)
```

This query displays only the current connections at the time of the query. The absence of results doesn't indicate that no applications are using SSL connections. Other SSL connections might be established at a different time.

Determining whether a client requires certificate verification in order to connect

When a client, such as `psql` or `JDBC`, is configured with SSL support, the client first tries to connect to the database with SSL by default. If the client can't connect with SSL, it reverts to connecting without SSL. The default `sslmode` mode used is different between libpq-based clients (such as `psql`) and `JDBC`. The libpq-based clients default to `prefer`, where `JDBC` clients default to `verify-full`. The certificate on the server is verified only when `sslrootcert` is provided with `sslmode` set to `require`, `verify-ca`, or `verify-full`. An error is thrown if the certificate is invalid.

Use PGSSLROOTCERT to verify the certificate with the PGSSLMODE environment variable, with PGSSLMODE set to require, verify-ca, or verify-full.

```
PGSSLMODE=require PGSSLROOTCERT=/fullpath/rds-ca-2019-root.pem psql -h pgdbidentifier.cxxxxxx.us-east-2.rds.amazonaws.com -U masteruser -d postgres
```

Use the sslrootcert argument to verify the certificate with sslmode in connection string format, with sslmode set to require, verify-ca, or verify-full to verify the certificate.

```
psql "host=pgdbidentifier.cxxxxxx.us-east-2.rds.amazonaws.com sslmode=require sslrootcert=/full/path/rds-ca-2019-root.pem user=masteruser dbname=postgres"
```

For example, in the preceding case, if you are using an invalid root certificate, then you see an error similar to the following on your client.

```
psql: SSL error: certificate verify failed
```

Updating your application trust store

For information about updating the trust store for PostgreSQL applications, see [Secure TCP/IP connections with SSL in the PostgreSQL documentation](#).

For information about downloading the root certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

For sample scripts that import certificates, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

When you update the trust store, you can retain older certificates in addition to adding the new certificates.

Using SSL/TLS connections for different types of applications

The following provides information about using SSL/TLS connections for different types of applications:

- **psql**

The client is invoked from the command line by specifying options either as a connection string or as environment variables. For SSL/TLS connections, the relevant options are sslmode (environment variable PGSSLMODE), sslrootcert (environment variable PGSSLROOTCERT).

For the complete list of options, see [Parameter key words](#) in the PostgreSQL documentation. For the complete list of environment variables, see [Environment variables](#) in the PostgreSQL documentation.

- **pgAdmin**

This browser-based client is a more user-friendly interface for connecting to a PostgreSQL database.

For information about configuring connections, see the [pgAdmin documentation](#).

- **JDBC**

JDBC enables database connections with Java applications.

For general information about connecting to a PostgreSQL database with JDBC, see [Connecting to the database](#) in the PostgreSQL JDBC driver documentation. For information about connecting with SSL/TLS, see [Configuring the client](#) in the PostgreSQL JDBC driver documentation.

- **Python**

A popular Python library for connecting to PostgreSQL databases is `psycopg2`.

For information about using `psycopg2`, see the [psycopg2 documentation](#). For a short tutorial on how to connect to a PostgreSQL database, see [Psycopg2 tutorial](#). You can find information about the options the `connect` command accepts in [The psycopg2 module content](#).

Important

After you have determined that your database connections use SSL/TLS and have updated your application trust store, you can update your database to use the rds-ca-2019 certificates. For instructions, see step 3 in [Updating your CA certificate by modifying your DB instance \(p. 2007\)](#).

Using Kerberos authentication with Amazon RDS for PostgreSQL

You can use Kerberos to authenticate users when they connect to your DB instance running PostgreSQL. To do so, you configure your DB instance to use AWS Directory Service for Microsoft Active Directory for Kerberos authentication. AWS Directory Service for Microsoft Active Directory is also called AWS Managed Microsoft AD. It's a feature available with AWS Directory Service. To learn more, see [What is AWS Directory Service?](#) in the *AWS Directory Service Administration Guide*.

You create an AWS Managed Microsoft AD directory to store user credentials. You then provide to your PostgreSQL DB instance the Active Directory's domain and other information. When users authenticate with the PostgreSQL DB instance, authentication requests are forwarded to the AWS Managed Microsoft AD directory.

Keeping all of your credentials in the same directory can save you time and effort. You have a centralized place for storing and managing credentials for multiple DB instances. Using a directory can also improve your overall security profile.

You can also access credentials from your own on-premises Microsoft Active Directory. To do so you create a trusting domain relationship so that the AWS Managed Microsoft AD directory trusts your on-premises Microsoft Active Directory. In this way, your users can access your PostgreSQL instances with the same Windows single sign-on (SSO) experience as when they access workloads in your on-premises network.

Topics

- [Region and version availability \(p. 1823\)](#)
- [Overview of Kerberos authentication for PostgreSQL DB instances \(p. 1823\)](#)
- [Setting up Kerberos authentication for PostgreSQL DB instances \(p. 1824\)](#)
- [Managing a DB instance in a Domain \(p. 1833\)](#)
- [Connecting to PostgreSQL with Kerberos authentication \(p. 1834\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability of RDS for PostgreSQL with Kerberos authentication, see [Kerberos authentication \(p. 101\)](#).

Overview of Kerberos authentication for PostgreSQL DB instances

To set up Kerberos authentication for a PostgreSQL DB instance, take the following steps, described in more detail later:

1. Use AWS Managed Microsoft AD to create an AWS Managed Microsoft AD directory. You can use the AWS Management Console, the AWS CLI, or the AWS Directory Service API to create the directory. Make sure to open the relevant outbound ports on the directory security group so that the directory can communicate with the instance.
2. Create a role that provides Amazon RDS access to make calls to your AWS Managed Microsoft AD directory. To do so, create an AWS Identity and Access Management (IAM) role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

For the IAM role to allow access, the AWS Security Token Service (AWS STS) endpoint must be activated in the correct AWS Region for your AWS account. AWS STS endpoints are active by default in all AWS Regions, and you can use them without any further actions. For more information, see [Activating and deactivating AWS STS in an AWS Region](#) in the *IAM User Guide*.

3. Create and configure users in the AWS Managed Microsoft AD directory using the Microsoft Active Directory tools. For more information about creating users in your Active Directory, see [Manage users and groups in AWS Managed Microsoft AD](#) in the *AWS Directory Service Administration Guide*.
4. If you plan to locate the directory and the DB instance in different AWS accounts or virtual private clouds (VPCs), configure VPC peering. For more information, see [What is VPC peering?](#) in the *Amazon VPC Peering Guide*.
5. Create or modify a PostgreSQL DB instance either from the console, CLI, or RDS API using one of the following methods:
 - [Creating an Amazon RDS DB instance](#) (p. 230)
 - [Modifying an Amazon RDS DB instance](#) (p. 327)
 - [Restoring from a DB snapshot](#) (p. 452)
 - [Restoring a DB instance to a specified time](#) (p. 499)

You can locate the instance in the same Amazon Virtual Private Cloud (VPC) as the directory or in a different AWS account or VPC. When you create or modify the PostgreSQL DB instance, do the following:

- Provide the domain identifier (d-* identifier) that was generated when you created your directory.
 - Provide the name of the IAM role that you created.
 - Ensure that the DB instance security group can receive inbound traffic from the directory security group.
6. Use the RDS master user credentials to connect to the PostgreSQL DB instance. Create the user in PostgreSQL to be identified externally. Externally identified users can log in to the PostgreSQL DB instance using Kerberos authentication.

Setting up Kerberos authentication for PostgreSQL DB instances

You use AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) to set up Kerberos authentication for a PostgreSQL DB instance. To set up Kerberos authentication, take the following steps.

Topics

- [Step 1: Create a directory using AWS Managed Microsoft AD](#) (p. 1825)
- [Step 2: \(Optional\) Create a trust relationship between your on-premises Active Directory and AWS Directory Service](#) (p. 1828)
- [Step 3: Create an IAM role for Amazon RDS to access the AWS Directory Service](#) (p. 1829)
- [Step 4: Create and configure users](#) (p. 1830)
- [Step 5: Enable cross-VPC traffic between the directory and the DB instance](#) (p. 1830)
- [Step 6: Create or modify a PostgreSQL DB instance](#) (p. 1831)
- [Step 7: Create PostgreSQL users for your Kerberos principals](#) (p. 1832)
- [Step 8: Configure a PostgreSQL client](#) (p. 1833)

Step 1: Create a directory using AWS Managed Microsoft AD

AWS Directory Service creates a fully managed Active Directory in the AWS Cloud. When you create an AWS Managed Microsoft AD directory, AWS Directory Service creates two domain controllers and DNS servers for you. The directory servers are created in different subnets in a VPC. This redundancy helps make sure that your directory remains accessible even if a failure occurs.

When you create an AWS Managed Microsoft AD directory, AWS Directory Service performs the following tasks on your behalf:

- Sets up an Active Directory within your VPC.
- Creates a directory administrator account with the user name Admin and the specified password. You use this account to manage your directory.

Important

Make sure to save this password. AWS Directory Service doesn't store this password, and it can't be retrieved or reset.

- Creates a security group for the directory controllers. The security group must permit communication with the PostgreSQL DB instance.

When you launch AWS Directory Service for Microsoft Active Directory, AWS creates an Organizational Unit (OU) that contains all of your directory's objects. This OU, which has the NetBIOS name that you entered when you created your directory, is located in the domain root. The domain root is owned and managed by AWS.

The Admin account that was created with your AWS Managed Microsoft AD directory has permissions for the most common administrative activities for your OU:

- Create, update, or delete users
- Add resources to your domain such as file or print servers, and then assign permissions for those resources to users in your OU
- Create additional OUs and containers
- Delegate authority
- Restore deleted objects from the Active Directory Recycle Bin
- Run Active Directory and Domain Name Service (DNS) modules for Windows PowerShell on the Active Directory Web Service

The Admin account also has rights to perform the following domain-wide activities:

- Manage DNS configurations (add, remove, or update records, zones, and forwarders)
- View DNS event logs
- View security event logs

To create a directory with AWS Managed Microsoft AD

1. In the [AWS Directory Service console](#) navigation pane, choose **Directories**, and then choose **Set up directory**.
2. Choose **AWS Managed Microsoft AD**. AWS Managed Microsoft AD is the only option currently supported for use with Amazon RDS.
3. Choose **Next**.
4. On the **Enter directory information** page, provide the following information:

Edition

Choose the edition that meets your requirements.

Directory DNS name

The fully qualified name for the directory, such as **corp.example.com**.

Directory NetBIOS name

An optional short name for the directory, such as CORP.

Directory description

An optional description for the directory.

Admin password

The password for the directory administrator. The directory creation process creates an administrator account with the user name Admin and this password.

The directory administrator password can't include the word "admin." The password is case-sensitive and must be 8–64 characters in length. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a–z)
- Uppercase letters (A–Z)
- Numbers (0–9)
- Nonalphanumeric characters (~!@#\$%^&*_+=`|\{\}[];'"<>,./?)

Confirm password

Retype the administrator password.

Important

Make sure that you save this password. AWS Directory Service doesn't store this password, and it can't be retrieved or reset.

5. Choose **Next**.
6. On the **Choose VPC and subnets** page, provide the following information:

VPC

Choose the VPC for the directory. You can create the PostgreSQL DB instance in this same VPC or in a different VPC.

Subnets

Choose the subnets for the directory servers. The two subnets must be in different Availability Zones.

7. Choose **Next**.
8. Review the directory information. If changes are needed, choose **Previous** and make the changes. When the information is correct, choose **Create directory**.

Review & create

Review

Directory type	VPC
Microsoft AD	vpc-8b6b78e9 ([REDACTED])
Directory DNS name	Subnets
corp.example.com	subnet-75128d10 ([REDACTED], us-east-1a) subnet-f51665dd ([REDACTED], us-east-1b)
Directory NetBIOS name	
CORP	
Directory description	
My directory	

Pricing

Edition	Free trial eligible Learn more 30-day limited trial
Standard	
~USD [REDACTED] *	
* Includes two domain controllers, USD [REDACTED] /mo for each additional domain controller.	

[Cancel](#) [Previous](#) [Create directory](#)

It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes to **Active**.

To see information about your directory, choose the directory ID in the directory listing. Make a note of the **Directory ID** value. You need this value when you create or modify your PostgreSQL DB instance.

The screenshot shows the 'Directory details' page for a Microsoft AD directory. The 'Directory ID' field, which contains the value 'd-90670a8d36', is circled in red. Other visible fields include 'Directory type' (Microsoft AD), 'Edition' (Standard), 'VPC' (vpc-6594f31c), 'Status' (Active), 'Subnets' (subnet-7d36a227, subnet-a2ab49c6), 'Last updated' (Tuesday, January 7, 2020), 'Availability zones' (us-east-1c, us-east-1d), 'Launch time' (Tuesday, January 7, 2020), 'DNS address' (redacted), 'Directory DNS name' (corp.example.com), 'Directory NetBIOS name' (CORP), and 'Description' (My directory). Below the table, there are tabs for 'Application management' (which is selected), 'Scale & share', 'Networking & security', and 'Maintenance'.

Step 2: (Optional) Create a trust relationship between your on-premises Active Directory and AWS Directory Service

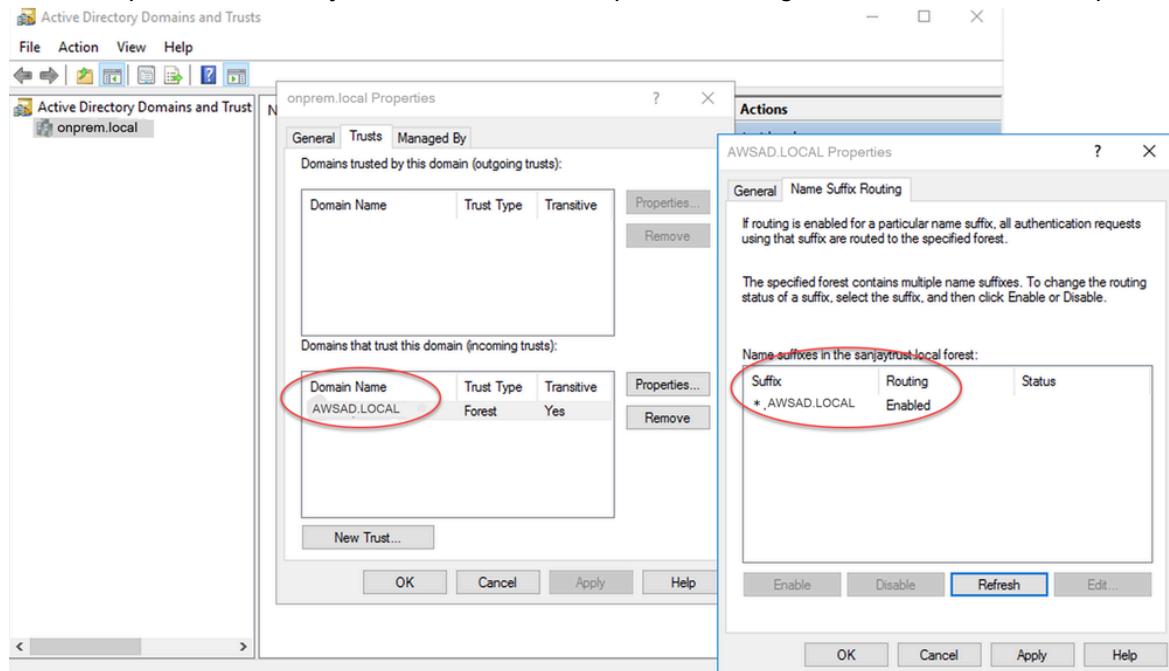
If you don't plan to use your own on-premises Microsoft Active Directory, skip to [Step 3: Create an IAM role for Amazon RDS to access the AWS Directory Service \(p. 1829\)](#).

To get Kerberos authentication using your on-premises Active Directory, you need to create a trusting domain relationship using a forest trust between your on-premises Microsoft Active Directory and the AWS Managed Microsoft AD directory (created in [Step 1: Create a directory using AWS Managed Microsoft AD \(p. 1825\)](#)). The trust can be one-way, where the AWS Managed Microsoft AD directory trusts the on-premises Microsoft Active Directory. The trust can also be two-way, where both Active Directories trust each other. For more information about setting up trusts using AWS Directory Service, see [When to create a trust relationship](#) in the *AWS Directory Service Administration Guide*.

Note

If you use an on-premises Microsoft Active Directory, Windows clients connect using the domain name of the AWS Directory Service in the endpoint rather than rds.amazonaws.com. To learn more, see [Connecting to PostgreSQL with Kerberos authentication \(p. 1834\)](#).

Make sure that your on-premises Microsoft Active Directory domain name includes a DNS suffix routing that corresponds to the newly created trust relationship. The following screenshot shows an example.



Step 3: Create an IAM role for Amazon RDS to access the AWS Directory Service

For Amazon RDS to call AWS Directory Service for you, your AWS account needs an IAM role that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`. This role allows Amazon RDS to make calls to AWS Directory Service.

When you create a DB instance using the AWS Management Console and your console user account has the `iam:CreateRole` permission, the console creates the needed IAM role automatically. In this case, the role name is `rds-directoryservice-kerberos-access-role`. Otherwise, you must create the IAM role manually. When you create this IAM role, choose `Directory Service`, and attach the AWS managed policy `AmazonRDSDirectoryServiceAccess` to it.

For more information about creating IAM roles for a service, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Note

The IAM role used for Windows Authentication for RDS for Microsoft SQL Server can't be used for Amazon RDS for PostgreSQL.

As an alternative to using the `AmazonRDSDirectoryServiceAccess` managed policy, you can create policies with the required permissions. In this case, the IAM role must have the following IAM trust policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",

```

```
        "rds.amazonaws.com"
    ],
},
"Action": "sts:AssumeRole"
}
]
```

The role must also have the following IAM role policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Step 4: Create and configure users

You can create users by using the Active Directory Users and Computers tool. This is one of the Active Directory Domain Services and Active Directory Lightweight Directory Services tools. For more information, see [Add Users and Computers to the Active Directory domain](#) in the Microsoft documentation. In this case, users are individuals or other entities, such as their computers that are part of the domain and whose identities are being maintained in the directory.

To create users in an AWS Directory Service directory, you must be connected to a Windows-based Amazon EC2 instance that's a member of the AWS Directory Service directory. At the same time, you must be logged in as a user that has privileges to create users. For more information, see [Create a user](#) in the *AWS Directory Service Administration Guide*.

Step 5: Enable cross-VPC traffic between the directory and the DB instance

If you plan to locate the directory and the DB instance in the same VPC, skip this step and move on to [Step 6: Create or modify a PostgreSQL DB instance \(p. 1831\)](#).

If you plan to locate the directory and the DB instance in different VPCs, configure cross-VPC traffic using VPC peering or [AWS Transit Gateway](#).

The following procedure enables traffic between VPCs using VPC peering. Follow the instructions in [What is VPC peering?](#) in the *Amazon Virtual Private Cloud Peering Guide*.

To enable cross-VPC traffic using VPC peering

1. Set up appropriate VPC routing rules to ensure that network traffic can flow both ways.
2. Ensure that the DB instance security group can receive inbound traffic from the directory security group.
3. Ensure that there is no network access control list (ACL) rule to block traffic.

If a different AWS account owns the directory, you must share the directory.

To share the directory between AWS accounts

1. Start sharing the directory with the AWS account that the DB instance will be created in by following the instructions in [Tutorial: Sharing your AWS Managed Microsoft AD directory for seamless EC2 Domain-join](#) in the *AWS Directory Service Administration Guide*.
2. Sign in to the AWS Directory Service console using the account for the DB instance, and ensure that the domain has the SHARED status before proceeding.
3. While signed into the AWS Directory Service console using the account for the DB instance, note the **Directory ID** value. You use this directory ID to join the DB instance to the domain.

Step 6: Create or modify a PostgreSQL DB instance

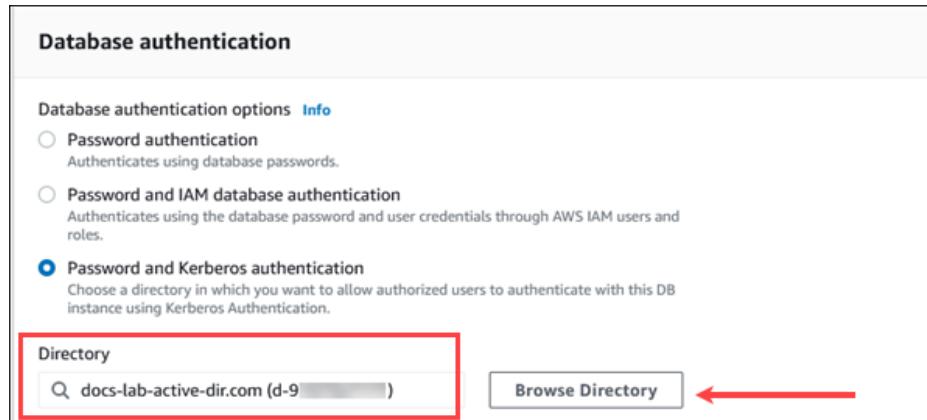
Create or modify a PostgreSQL DB instance for use with your directory. You can use the console, CLI, or RDS API to associate a DB instance with a directory. You can do this in one of the following ways:

- Create a new PostgreSQL DB instance using the console, the [create-db-instance](#) CLI command, or the [CreateDBInstance](#) RDS API operation. For instructions, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- Modify an existing PostgreSQL DB instance using the console, the [modify-db-instance](#) CLI command, or the [ModifyDBInstance](#) RDS API operation. For instructions, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- Restore a PostgreSQL DB instance from a DB snapshot using the console, the [restore-db-instance-from-db-snapshot](#) CLI command, or the [RestoreDBInstanceFromDBSnapshot](#) RDS API operation. For instructions, see [Restoring from a DB snapshot \(p. 452\)](#).
- Restore a PostgreSQL DB instance to a point-in-time using the console, the [restore-db-instance-to-point-in-time](#) CLI command, or the [RestoreDBInstanceToPointInTime](#) RDS API operation. For instructions, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Kerberos authentication is only supported for PostgreSQL DB instances in a VPC. The DB instance can be in the same VPC as the directory, or in a different VPC. The DB instance must use a security group that allows ingress and egress within the directory's VPC so the DB instance can communicate with the directory.

Console

When you use the console to create, modify, or restore a DB instance, choose **Password and Kerberos authentication** in the **Database authentication** section. Then choose **Browse Directory**. Select the directory or choose **Create a new directory** to use the Directory Service.



AWS CLI

When you use the AWS CLI, the following parameters are required for the DB instance to be able to use the directory that you created:

- For the `--domain` parameter, use the domain identifier ("d-*" identifier) generated when you created the directory.
- For the `--domain-iam-role-name` parameter, use the role you created that uses the managed IAM policy `AmazonRDSDirectoryServiceAccess`.

For example, the following CLI command modifies a DB instance to use a directory.

```
aws rds modify-db-instance --db-instance-identifier mydbinstance --domain d-Directory-ID --domain-iam-role-name role-name
```

Important

If you modify a DB instance to enable Kerberos authentication, reboot the DB instance after making the change.

Step 7: Create PostgreSQL users for your Kerberos principals

At this point, your RDS for PostgreSQL DB instance is joined to the AWS Managed Microsoft AD domain. The users that you created in the directory in [Step 4: Create and configure users \(p. 1830\)](#) need to be set up as PostgreSQL database users and granted privileges to login to the database. You do that by signing in as the database user with `rds_superuser` privileges. For example, if you accepted the defaults when you created your RDS for PostgreSQL DB instance, you use `postgres`, as shown in the following steps.

To create PostgreSQL database users for Kerberos principals

1. Use `psql` to connect to your RDS for PostgreSQL DB instance endpoint using `psql`. The following example uses the default `postgres` account for the `rds_superuser` role.

```
psql --host=cluster-instance-1.1112222333.aws-region.rds.amazonaws.com --port=5432 --username=postgres --password
```

2. Create a database user name for each Kerberos principal (Active Directory username) that you want to have access to the database. Use the canonical username (identity) as defined in the Active Directory instance, that is, a lower-case alias (username in Active Directory) and the upper-case name of the Active Directory domain for that user name. The Active Directory user name is an externally authenticated user, so use quotes around the name as shown following.

```
postgres=> CREATE USER "username@CORP.EXAMPLE.COM" WITH LOGIN;  
CREATE ROLE
```

3. Grant the `rds_ad` role to the database user.

```
postgres=> GRANT rds_ad TO "username@CORP.EXAMPLE.COM";  
GRANT ROLE
```

After you finish creating all the PostgreSQL users for your Active Directory user identities, users can access the RDS for PostgreSQL DB instance by using their Kerberos credentials.

It's assumed that the database users who authenticate using Kerberos are doing so from client machines that are members of the Active Directory domain.

Database users that have been granted the `rds_ad` role can't also have the `rds_iam` role. This also applies to nested memberships. For more information, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

Step 8: Configure a PostgreSQL client

To configure a PostgreSQL client, take the following steps:

- Create a `krb5.conf` file (or equivalent) to point to the domain.
- Verify that traffic can flow between the client host and AWS Directory Service. Use a network utility such as Netcat for the following:
 - Verify traffic over DNS for port 53.
 - Verify traffic over TCP/UDP for port 53 and for Kerberos, which includes ports 88 and 464 for AWS Directory Service.
- Verify that traffic can flow between the client host and the DB instance over the database port. For example, use `psql` to connect and access the database.

The following is sample `krb5.conf` content for AWS Managed Microsoft AD.

```
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
    kdc = example.com
    admin_server = example.com
}
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

The following is sample `krb5.conf` content for an on-premises Microsoft Active Directory.

```
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
    kdc = example.com
    admin_server = example.com
}
ONPREM.COM = {
    kdc = onprem.com
    admin_server = onprem.com
}
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
.onprem.com = ONPREM.COM
onprem.com = ONPREM.COM
.rds.amazonaws.com = EXAMPLE.COM
.amazonaws.com.cn = EXAMPLE.COM
.amazon.com = EXAMPLE.COM
```

Managing a DB instance in a Domain

You can use the console, the CLI, or the RDS API to manage your DB instance and its relationship with your Microsoft Active Directory. For example, you can associate an Active Directory to enable Kerberos authentication. You can also remove the association for an Active Directory to disable Kerberos.

authentication. You can also move a DB instance to be externally authenticated by one Microsoft Active Directory to another.

For example, using the CLI, you can do the following:

- To reattempt enabling Kerberos authentication for a failed membership, use the [modify-db-instance](#) CLI command. Specify the current membership's directory ID for the --domain option.
- To disable Kerberos authentication on a DB instance, use the [modify-db-instance](#) CLI command. Specify none for the --domain option.
- To move a DB instance from one domain to another, use the [modify-db-instance](#) CLI command. Specify the domain identifier of the new domain for the --domain option.

Understanding Domain membership

After you create or modify your DB instance, it becomes a member of the domain. You can view the status of the domain membership in the console or by running the [describe-db-instances](#) CLI command. The status of the DB instance can be one of the following:

- `kerberos-enabled` – The DB instance has Kerberos authentication enabled.
- `enabling-kerberos` – AWS is in the process of enabling Kerberos authentication on this DB instance.
- `pending-enable-kerberos` – Enabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-enable-kerberos` – AWS will attempt to enable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `pending-disable-kerberos` – Disabling Kerberos authentication is pending on this DB instance.
- `pending-maintenance-disable-kerberos` – AWS will attempt to disable Kerberos authentication on the DB instance during the next scheduled maintenance window.
- `enable-kerberos-failed` – A configuration problem prevented AWS from enabling Kerberos authentication on the DB instance. Correct the configuration problem before reissuing the command to modify the DB instance.
- `disabling-kerberos` – AWS is in the process of disabling Kerberos authentication on this DB instance.

A request to enable Kerberos authentication can fail because of a network connectivity issue or an incorrect IAM role. In some cases, the attempt to enable Kerberos authentication might fail when you create or modify a DB instance. If so, make sure that you are using the correct IAM role, then modify the DB instance to join the domain.

Note

Only Kerberos authentication with RDS for PostgreSQL sends traffic to the domain's DNS servers. All other DNS requests are treated as outbound network access on your DB instances running PostgreSQL. For more information about outbound network access with RDS for PostgreSQL, see [Using a custom DNS server for outbound network access \(p. 1837\)](#).

Connecting to PostgreSQL with Kerberos authentication

You can connect to PostgreSQL with Kerberos authentication with the pgAdmin interface or with a command-line interface such as psql. For more information about connecting, see [Connecting to a DB instance running the PostgreSQL database engine \(p. 1809\)](#). For information about obtaining the endpoint, port number, and other details needed for connection, see [Using pgAdmin to connect to a PostgreSQL DB instance \(p. 192\)](#).

pgAdmin

To use pgAdmin to connect to PostgreSQL with Kerberos authentication, take the following steps:

1. Launch the pgAdmin application on your client computer.
2. On the **Dashboard** tab, choose **Add New Server**.
3. In the **Create - Server** dialog box, enter a name on the **General** tab to identify the server in pgAdmin.
4. On the **Connection** tab, enter the following information from your RDS for PostgreSQL database.
 - For **Host**, enter the endpoint for the RDS for PostgreSQL DB instance. An endpoint looks similar to the following:

```
RDS-DB-instance.111122223333.aws-region.rds.amazonaws.com
```

To connect to an on-premises Microsoft Active Directory from a Windows client, you use the domain name of the AWS Managed Active Directory instead of `rds.amazonaws.com` in the host endpoint. For example, suppose that the domain name for the AWS Managed Active Directory is `corp.example.com`. Then for **Host**, the endpoint would be specified as follows:

```
RDS-DB-instance.111122223333.aws-region.corp.example.com
```

- For **Port**, enter the assigned port.
 - For **Maintenance database**, enter the name of the initial database to which the client will connect.
 - For **Username**, enter the user name that you entered for Kerberos authentication in [Step 7: Create PostgreSQL users for your Kerberos principals \(p. 1832\)](#).
5. Choose **Save**.

Psql

To use psql to connect to PostgreSQL with Kerberos authentication, take the following steps:

1. At a command prompt, run the following command.

```
kinit username
```

Replace `username` with the user name. At the prompt, enter the password stored in the Microsoft Active Directory for the user.

2. If the PostgreSQL DB instance is using a publicly accessible VPC, put a private IP address for your DB instance endpoint in your `/etc/hosts` file on the EC2 client. For example, the following commands obtain the private IP address and then put it in the `/etc/hosts` file.

```
% dig +short PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com
;; Truncated, retrying in TCP mode.
ec2-34-210-197-118.AWS-Region.compute.amazonaws.com.
34.210.197.118

% echo " 34.210.197.118 PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com" >> /etc/
hosts
```

If you're using an on-premises Microsoft Active Directory from a Windows client, then you need to connect using a specialized endpoint. Instead of using the Amazon domain `rds.amazonaws.com` in the host endpoint, use the domain name of the AWS Managed Active Directory.

For example, suppose that the domain name for your AWS Managed Active Directory is `corp.example.com`. Then use the format `PostgreSQL-endpoint.AWS-Region.corp.example.com` for the endpoint and put it in the `/etc/hosts` file.

```
% echo " 34.210.197.118 PostgreSQL-endpoint.AWS-Region.corp.example.com" >> /etc/hosts
```

3. Use the following `psql` command to log in to a PostgreSQL DB instance that is integrated with Active Directory.

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com postgres
```

To log in to the PostgreSQL DB cluster from a Windows client using an on-premises Active Directory, use the following `psql` command with the domain name from the previous step (`corp.example.com`):

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-Region.corp.example.com postgres
```

Using a custom DNS server for outbound network access

RDS for PostgreSQL supports outbound network access on your DB instances and allows Domain Name Service (DNS) resolution from a custom DNS server owned by the customer. You can resolve only fully qualified domain names from your RDS for PostgreSQL DB instance through your custom DNS server.

Topics

- [Turning on custom DNS resolution \(p. 1837\)](#)
- [Turning off custom DNS resolution \(p. 1837\)](#)
- [Setting up a custom DNS server \(p. 1837\)](#)

Turning on custom DNS resolution

To turn on DNS resolution in your customer VPC, first associate a custom DB parameter group to your RDS for PostgreSQL instance. Then turn on the `rds.custom_dns_resolution` parameter by setting it to 1, and then restart the DB instance for the changes to take place.

Turning off custom DNS resolution

To turn off DNS resolution in your customer VPC, first turn off the `rds.custom_dns_resolution` parameter of your custom DB parameter group by setting it to 0. Then restart the DB instance for the changes to take place.

Setting up a custom DNS server

After you set up your custom DNS name server, it takes up to 30 minutes to propagate the changes to your DB instance. After the changes are propagated to your DB instance, all outbound network traffic requiring a DNS lookup queries your DNS server over port 53.

Note

If you don't set up a custom DNS server and `rds.custom_dns_resolution` is set to 1, hosts are resolved using an Amazon Route 53 private zone. For more information, see [Working with private hosted zones](#).

To set up a custom DNS server for your RDS for PostgreSQL DB instance

1. From the Dynamic Host Configuration Protocol (DHCP) options set attached to your VPC, set the `domain-name-servers` option to the IP address of your DNS name server. For more information, see [DHCP options sets](#).

Note

The `domain-name-servers` option accepts up to four values, but your Amazon RDS DB instance uses only the first value.

2. Ensure that your DNS server can resolve all lookup queries, including public DNS names, Amazon EC2 private DNS names, and customer-specific DNS names. If the outbound network traffic contains any DNS lookups that your DNS server can't handle, your DNS server must have appropriate upstream DNS providers configured.
3. Configure your DNS server to produce User Datagram Protocol (UDP) responses of 512 bytes or less.
4. Configure your DNS server to produce Transmission Control Protocol (TCP) responses of 1,024 bytes or less.

5. Configure your DNS server to allow inbound traffic from your Amazon RDS DB instances over port 53. If your DNS server is in an Amazon VPC, the VPC must have a security group that contains inbound rules that allow UDP and TCP traffic on port 53. If your DNS server is not in an Amazon VPC, it must have appropriate firewall settings to allow UDP and TCP inbound traffic on port 53.
For more information, see [Security groups for your VPC](#) and [Adding and removing rules](#).
6. Configure the VPC of your Amazon RDS DB instance to allow outbound traffic over port 53. Your VPC must have a security group that contains outbound rules that allow UDP and TCP traffic on port 53.
For more information, see [Security groups for your VPC](#) and [Adding and removing rules](#) in the [Amazon VPC User Guide](#).
7. Make sure that the routing path between the Amazon RDS DB instance and the DNS server is configured correctly to allow DNS traffic.
Also, if the Amazon RDS DB instance and the DNS server are not in the same VPC, make sure that a peering connection is set up between them. For more information, see [What is VPC peering?](#) in [Amazon VPC Peering Guide](#).

Upgrading the PostgreSQL DB engine for Amazon RDS

There are two types of upgrades you can manage for your PostgreSQL DB instance:

- Operating system updates – Occasionally, Amazon RDS might need to update the underlying operating system of your DB instance to apply security fixes or OS changes. You can decide when Amazon RDS applies OS updates by using the RDS console, AWS Command Line Interface (AWS CLI), or RDS API. For more information about OS updates, see [Applying updates for a DB instance \(p. 352\)](#).
- Database engine upgrades – When Amazon RDS supports a new version of a database engine, you can upgrade your DB instances to the new version.

When Amazon RDS supports a new version of a database engine, you can upgrade your DB instances to the new version. There are two kinds of upgrades for PostgreSQL DB instances: major version upgrades and minor version upgrades.

Major version upgrades

Major version upgrades can contain database changes that are not backward-compatible with existing applications. As a result, you must manually perform major version upgrades of your DB instances. You can initiate a major version upgrade by modifying your DB instance. However, before you perform a major version upgrade, we recommend that you follow the steps described in [Choosing a major version upgrade for PostgreSQL \(p. 1841\)](#). During a major version upgrade, Amazon RDS also upgrades all of your in-Region read replicas along with the primary DB instance.

Minor version upgrades

In contrast, *minor version upgrades* include only changes that are backward-compatible with existing applications. You can initiate a minor version upgrade manually by modifying your DB instance. Or you can enable the **Auto minor version upgrade** option when creating or modifying a DB instance. Doing so means that your DB instance is automatically upgraded after Amazon RDS tests and approves the new version. If your PostgreSQL DB instance is using read replicas, you must first upgrade all of the read replicas before upgrading the primary instance. If your DB instance is in a Multi-AZ deployment, then the writer and any standby replicas are upgraded simultaneously. Therefore, your DB instance might not be available until the upgrade is complete. For more details, see [Automatic minor version upgrades for PostgreSQL \(p. 1847\)](#). For information about manually performing a minor version upgrade, see [Manually upgrading the engine version \(p. 360\)](#).

For more information about database engine versions, and the policy for deprecating database engine versions, see [Database Engine Versions in the Amazon RDS FAQs](#).

Topics

- [Overview of upgrading PostgreSQL \(p. 1840\)](#)
- [PostgreSQL version numbers \(p. 1841\)](#)
- [Choosing a major version upgrade for PostgreSQL \(p. 1841\)](#)
- [How to perform a major version upgrade \(p. 1843\)](#)
- [Automatic minor version upgrades for PostgreSQL \(p. 1847\)](#)
- [Upgrading PostgreSQL extensions \(p. 1849\)](#)

Overview of upgrading PostgreSQL

To safely upgrade your DB instances, Amazon RDS uses the pg_upgrade utility described in the [PostgreSQL documentation](#).

When you use the AWS Management Console to upgrade a DB instance, it shows the valid upgrade targets for the DB instance. You can also use the following AWS CLI command to identify the valid upgrade targets for a DB instance:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version version-number \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version version-number ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

For example, to identify the valid upgrade targets for a PostgreSQL version 10.11 DB instance, run the following AWS CLI command:

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version 10.11 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version 10.11 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

If your backup retention period is greater than 0, Amazon RDS takes two DB snapshots during the upgrade process. The first DB snapshot is of the DB instance before any upgrade changes have been made. If the upgrade doesn't work for your databases, you can restore this snapshot to create a DB instance running the old version. The second DB snapshot is taken after the upgrade completes.

Note

Amazon RDS takes DB snapshots during the upgrade process only if you have set the backup retention period for your DB instance to a number greater than 0. To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

When you perform a major version upgrade of the primary DB instance, all the in-Region read replicas are also automatically upgraded. After the upgrade workflow starts, the read replicas wait for the pg_upgrade to complete successfully on the primary DB instance. Then the primary DB instance upgrade waits for the read replica upgrades to complete. You experience an outage until the upgrade is complete.

If your DB instance is in a Multi-AZ deployment, both the primary writer DB instance and standby DB instances are upgraded. The writer and standby DB instances are upgraded at the same time.

After an upgrade is complete, you can't revert to the previous version of the database engine. If you want to return to the previous version, restore the DB snapshot that was taken before the upgrade to create a new DB instance.

PostgreSQL version numbers

The version numbering sequence for the PostgreSQL database engine is as follows:

- For PostgreSQL versions 10 and later, the engine version number is in the form *major.minor*. The major version number is the integer part of the version number. The minor version number is the fractional part of the version number.

A major version upgrade increases the integer part of the version number, such as upgrading from *10.minor* to *11.minor*.

- For PostgreSQL versions earlier than 10, the engine version number is in the form *major.major.minor*. The major engine version number is both the integer and the first fractional part of the version number. For example, 9.6 is a major version. The minor version number is the third part of the version number. For example, for version 9.6.12, the 12 is the minor version number.

A major version upgrade increases the major part of the version number. For example, an upgrade from 9.6.12 to 10.11 is a major version upgrade, where 9.6 and 10 are the major version numbers.

Choosing a major version upgrade for PostgreSQL

Major version upgrades can contain changes that are not backward-compatible with previous versions of the database. New functionality can cause your existing applications to stop working correctly. For this reason, Amazon RDS doesn't apply major version upgrades automatically. To perform a major version upgrade, you modify your DB instance manually. Make sure that you thoroughly test any upgrade to verify that your applications work correctly before applying the upgrade to your production DB instances. When you do a PostgreSQL major version upgrade, we recommend that you follow the steps described in [How to perform a major version upgrade \(p. 1843\)](#).

When you upgrade a PostgreSQL DB instance to its next major version, any read replicas associated with the DB instance are also upgraded to that next major version. In some cases, you can skip to a higher major version when upgrading. If your upgrade skips a major version, the read replicas are also upgraded to that target major version. Upgrades to version 11 that skip other major versions have certain limitations. You can find the details in the steps described in [How to perform a major version upgrade \(p. 1843\)](#).

Most PostgreSQL extensions aren't upgraded during a PostgreSQL engine upgrade. These must be upgraded separately. For more information, see [Upgrading PostgreSQL extensions \(p. 1849\)](#).

You can find out which major versions are available for your RDS for PostgreSQL DB instance by running the following AWS CLI query:

```
aws rds describe-db-engine-versions --engine postgres --engine-version your-version --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --output text
```

The following table summarizes the results of this query for all available versions. An asterisk (*) on the version number means that version is deprecated. If your current version is deprecated, we recommend that you upgrade to the newest minor version upgrade target or to one of the other

available upgrade targets for that version. For more information about RDS for PostgreSQL 9.6 deprecation, see [Deprecation of PostgreSQL version 10 \(p. 1806\)](#).

Current source version (*deprec	Newest minor version upgrade target	Newest major version upgrade target	Other available upgrade targets									
14.4		14.5										
14.3		14.5	14.4									
14.2		14.5	14.4	14.3								
14.1		14.5	14.4	14.3	14.2							
13.8		14.5	14.4	14.3	14.2							
13.7		14.5	14.4	14.3	14.2							
13.6		14.5	14.4	14.3	14.2	13.7						
13.5		14.5	14.4	14.3	14.2	14.1	13.8	13.7	13.6			
13.4		14.5	14.4	14.3	14.2	14.1	13.8	13.7	13.6	13.5		
13.3		14.5	14.4	14.3	14.2	14.1	13.8	13.7	13.6	13.5	13.4	
13.2*, 13.1*	13.8	14.5	14.4	14.3	14.2	14.1	13.8	13.7	13.6	13.5	13.4	
12.12		14.5	13.8									
12.11		14.4	14.3	13.8	13.7	12.12						
12.10		14.2	13.8	13.7	13.6	12.12	12.11					
12.9		14.1	13.8	13.7	13.6	13.5	12.12	12.11	12.10			
12.8		13.8	13.7	13.6	13.5	13.4	12.12	12.11	12.10	12.9		
12.7		13.8	13.7	13.6	13.5	13.4	13.3	12.12	12.11	12.10	12.9	
12.6*, 12.5*, 12.4*, 12.3*, 12.2*, 12.1*	12.12	13.7	13.6	12.11	12.10	12.9	12.8	12.7				
11.17		14.5	13.8	12.12								
11.16		14.4	14.3	13.7	12.12	12.11	11.17					
11.15		14.2	13.6	12.12	12.11	12.10	11.17	11.16				
11.14		14.1	13.5	12.12	12.11	12.10	12.9	11.17	11.16	11.15		
11.13		13.4	12.12	12.11	12.10	12.9	12.8	11.17	11.16	11.15	11.14	
11.12		13.3	12.12	12.11	12.10	12.9	12.8	12.7	11.17	11.16	11.15	

Current source version (*deprec)	Newest minor version upgrade target	Newest major version upgrade target	Other available upgrade targets									
			14.5	13.8	12.12	11.17						
10.22		14.5	13.8	12.12	11.17							
10.21		14.3	13.7	12.11	11.17	11.16	10.22					
10.20		14.2	13.6	12.10	11.17	11.16	11.15	10.22	10.21			
10.19		14.1	13.5	12.9	11.17	11.16	11.15	11.14	10.20	10.22	10.21	
10.18		13.4	12.8	11.17	11.16	11.15	11.14	11.13	10.22	10.21	10.20	
10.17		13.3	12.7	11.17	11.16	11.15	11.14	11.13	11.12	10.22	10.21	
9.6.24		14.1	13.5	12.9	11.14	10.20	10.19					
9.6.23		13.4	12.8	11.13	10.20	10.19	10.18	9.6.24				
9.6.22		13.3	12.7	11.12	10.20	10.19	10.18	10.17	9.6.24	9.6.23		
9.6.19*, 9.6.18*, 9.6.17*, 9.6.16*, 9.6.15*, 9.6.14*, 9.6.12*, 9.6.11*, 9.6.10*, 9.6.9*, 9.6.8*, 9.6.6*, 9.6.5*, 9.6.3*, 9.6.2*, 9.6.1*	9.6.24	14.1	13.5	12.9	11.14	10.20	10.19	9.6.23	9.6.22			

How to perform a major version upgrade

We recommend the following process when upgrading an Amazon RDS PostgreSQL DB instance:

1. **Have a version-compatible parameter group ready** – If you are using a custom parameter group, you have two options. You can specify a default parameter group for the new DB engine version. Or you can create your own custom parameter group for the new DB engine version. For more information, see [Working with parameter groups \(p. 289\)](#)
2. **Check for unsupported DB instance classes** – Check that your database's instance class is compatible with the PostgreSQL version you are upgrading to. For more information, see [Supported DB engines for DB instance classes \(p. 12\)](#).
3. **Check for unsupported usage:**
 - **Prepared transactions** – Commit or roll back all open prepared transactions before attempting an upgrade.

You can use the following query to verify that there are no open prepared transactions on your instance.

```
SELECT count(*) FROM pg_catalog.pg_prepared_xacts;
```

- **Reg* data types** – Remove all uses of the *reg** data types before attempting an upgrade. Except for *regtype* and *regclass*, you can't upgrade the *reg** data types. The *pg_upgrade* utility can't persist this data type, which is used by Amazon RDS to do the upgrade.

To verify that there are no uses of unsupported *reg** data types, use the following query for each database.

```
SELECT count(*) FROM pg_catalog.pg_class c, pg_catalog.pg_namespace n,
pg_catalog.pg_attribute a
WHERE c.oid = a.attrelid
AND NOT a.attisdropped
AND a.atttypid IN ('pg_catalog.regproc'::pg_catalog.regtype,
'pg_catalog.regprocedure'::pg_catalog.regtype,
'pg_catalog.regoper'::pg_catalog.regtype,
'pg_catalog.regoperator'::pg_catalog.regtype,
'pg_catalog.regconfig'::pg_catalog.regtype,
'pg_catalog.regdictionary'::pg_catalog.regtype)
AND c.relnamespace = n.oid
AND n.nspname NOT IN ('pg_catalog', 'information_schema');
```

4. **Handle logical replication slots** – An upgrade can't occur if the instance has any logical replication slots. Logical replication slots are typically used for AWS DMS migration and for replicating tables from the database to data lakes, BI tools, and other targets. Before upgrading, make sure that you know the purpose of any logical replication slots that are in use, and confirm that it's okay to delete them. If the logical replication slots are still being used, you shouldn't delete them, and you can't proceed with the upgrade.

If the logical replication slots aren't needed, you can delete them using the following SQL:

```
SELECT * FROM pg_replication_slots;
SELECT pg_drop_replication_slot(slot_name);
```

Logical replication setups that use the *pglogical* extension also need to have slots dropped for a successful major version upgrade. For information about how to identify and drop slots created using the *pglogical* extension, see [Managing logical replication slots for RDS for PostgreSQL \(p. 1974\)](#).

5. **Handle read replicas** – An upgrade also upgrades the in-Region read replicas along with the primary DB instance.

You can't upgrade read replicas separately. If you could, it could lead to situations where the primary and replica DB instances have different PostgreSQL major versions. However, read replica upgrades might increase downtime on the primary DB instance. To prevent a read replica upgrade, promote the replica to a standalone instance or delete it before starting the upgrade process.

The upgrade process recreates the read replica's parameter group based on the read replica's current parameter group. You can apply a custom parameter group to a read replica only after the upgrade completes by modifying the read replica. For more information about read replicas, see [Working with read replicas for Amazon RDS for PostgreSQL \(p. 1852\)](#).

6. **Perform a backup** – We recommend that you perform a backup before performing the major version upgrade so that you have a known restore point for your database. If your backup retention period is greater than 0, the upgrade process creates DB snapshots of your DB instance before and after upgrading. To change your backup retention period, see [Modifying an Amazon RDS DB instance \(p. 327\)](#). To perform a backup manually, see [Creating a DB snapshot \(p. 448\)](#).

7. Upgrade certain extensions before a major version upgrade – If you plan to skip a major version with the upgrade, you need to update certain extensions *before* performing the major version upgrade. For example, upgrading from versions 9.5.x or 9.6.x to version 11.x skips a major version. The extensions to update include PostGIS and related extensions for processing spatial data.

- address_standardizer
- address_standardizer_data_us
- postgis
- postgis_tiger_geocoder
- postgis_topology

Run the following command for each extension that you're using:

```
ALTER EXTENSION PostgreSQL-extension UPDATE TO 'new-version'
```

For more information, see [Upgrading PostgreSQL extensions \(p. 1849\)](#). To learn more about upgrading PostGIS, see [Step 6: Upgrade the PostGIS extension \(p. 1983\)](#).

8. Drop certain extensions before the major version upgrade – An upgrade that skips a major version to version 11.x doesn't support updating the pgRouting extension. Upgrading from versions 9.4.x, 9.5.x, or 9.6.x to versions 11.x skip a major version. It's safe to drop the pgRouting extension and then reinstall it to a compatible version after the upgrade. For the extension versions you can update to, see [Supported PostgreSQL extension versions \(p. 1807\)](#).

The tsearch2 and chkpass extensions are no longer supported for PostgreSQL versions 11 or later. If you are upgrading to version 11.x, drop the tsearch2, and chkpass extensions before the upgrade.

9. Drop unknown data types – Drop unknown data types depending on the target version.

PostgreSQL version 10 stopped supporting the unknown data type. If a version 9.6 database uses the unknown data type, an upgrade to a version 10 shows an error message such as the following:

```
Database instance is in a state that cannot be upgraded: PreUpgrade checks failed:  
The instance could not be upgraded because the 'unknown' data type is used in user  
tables.  
Please remove all usages of the 'unknown' data type and try again."
```

To find the unknown data type in your database so you can remove the offending column or change it to a supported data type, use the following SQL:

```
SELECT DISTINCT data_type FROM information_schema.columns WHERE data_type ILIKE  
'unknown';
```

10 Perform an upgrade dry run – We highly recommend testing a major version upgrade on a duplicate of your production database before attempting the upgrade on your production database. To create a duplicate test instance, you can either restore your database from a recent snapshot or do a point-in-time restore of your database to its latest restorable time. For more information, see [Restoring from a snapshot \(p. 454\)](#) or [Restoring a DB instance to a specified time \(p. 499\)](#). For details on performing the upgrade, see [Manually upgrading the engine version \(p. 360\)](#).

In upgrading a version 9.6 DB instance to version 10, be aware that PostgreSQL 10 enables parallel queries by default. You can test the impact of parallelism *before* the upgrade by changing the max_parallel_workers_per_gather parameter on your test DB instance to 2.

Note

The default value for max_parallel_workers_per_gather parameter in the default.postgresql10 DB parameter group is 2.

For more information, see [Parallel Query](#) in the PostgreSQL documentation. To disable parallelism on version 10, set the `max_parallel_workers_per_gather` parameter to 0.

During the major version upgrade, the `public` and `template1` databases and the `public` schema in every database on the instance are temporarily renamed. These objects appear in the logs with their original name and a random string appended. The string is appended so that custom settings such as `locale` and `owner` are preserved during the major version upgrade. After the upgrade completes, the objects are renamed back to their original names.

Note

During the major version upgrade process, you can't do a point-in-time restore of your instance. After Amazon RDS performs the upgrade, it takes an automatic backup of the instance. You can perform a point-in-time restore to times before the upgrade began and after the automatic backup of your instance has completed.

11 If an upgrade fails with precheck procedure errors, resolve the issues – During the major version upgrade process, Amazon RDS for PostgreSQL first runs a precheck procedure to identify any issues that might cause the upgrade to fail. The precheck procedure checks all potential incompatible conditions across all databases in the instance.

If the precheck encounters an issue, it creates a log event indicating the upgrade precheck failed. The precheck process details are in an upgrade log named `pg_upgrade_precheck.log` for all the databases of a DB instance. Amazon RDS appends a timestamp to the file name. For more information about viewing logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

If a read replica upgrade fails at precheck, replication on the failed read replica is broken and the read replica is put in the terminated state. Delete the read replica and recreate a new read replica based on the upgraded primary DB instance.

Resolve all of the issues identified in the precheck log and then retry the major version upgrade. The following is an example of a precheck log.

```
-----  
Upgrade could not be run on Wed Apr 4 18:30:52 2018  
-----  
The instance could not be upgraded from 9.6.11 to 10.6 for the following reasons.  
Please take appropriate action on databases that have usage incompatible with the  
requested major engine version upgrade and try the upgrade again.  
  
* There are uncommitted prepared transactions. Please commit or rollback all prepared  
transactions.* One or more role names start with 'pg_'. Rename all role names that  
start with 'pg_'.  
  
* The following issues in the database 'my"million$"db' need to be corrected before  
upgrading:** The ["line","reg*"] data types are used in user tables. Remove all usage  
of these data types.  
** The database name contains characters that are not supported by RDS for PostgreSQL.  
Rename the database.  
** The database has extensions installed that are not supported on the target database  
version. Drop the following extensions from your database: ["tsearch2"].  
  
* The following issues in the database 'mydb' need to be corrected before upgrading:**  
The database has views or materialized views that depend on 'pg_stat_activity'. Drop  
the views.
```

12 If a read replica upgrade fails while upgrading the database, resolve the issue – A failed read replica is placed in the `incompatible-restore` state and replication is terminated on the DB instance. Delete the read replica and recreate a new read replica based on the upgraded primary DB instance.

A read replica upgrade might fail for the following reasons:

- It was unable to catch up with the primary DB instance even after a wait time.

- It was in a terminal or incompatible lifecycle state such as storage-full, incompatible-restore, and so on.
- When the primary DB instance upgrade started, there was a separate minor version upgrade running on the read replica.
- The read replica used incompatible parameters.
- The read replica was unable to communicate with the primary DB instance to synchronize the data folder.

13 Upgrade your production instance – When the dry-run major version upgrade is successful, you should be able to upgrade your production database with confidence. For more information, see [Manually upgrading the engine version \(p. 360\)](#).

14 Run the ANALYZE operation to refresh the pg_statistic table. You should do this for every database on all your PostgreSQL DB instances. Optimizer statistics aren't transferred during a major version upgrade, so you need to regenerate all statistics to avoid performance issues. Run the command without any parameters to generate statistics for all regular tables in the current database, as follows:

```
ANALYZE VERBOSE
```

The `VERBOSE` flag is optional, but using it shows you the progress. For more information, see [ANALYZE](#) in the PostgreSQL documentation.

Note

Run `ANALYZE` on your system after the upgrade to avoid performance issues.

After the major version upgrade is complete, we recommend the following:

- A PostgreSQL upgrade doesn't upgrade any PostgreSQL extensions. To upgrade extensions, see [Upgrading PostgreSQL extensions \(p. 1849\)](#).
- Optionally, use Amazon RDS to view two logs that the `pg_upgrade` utility produces. These are `pg_upgrade_internal.log` and `pg_upgrade_server.log`. Amazon RDS appends a timestamp to the file name for these logs. You can view these logs as you can any other log. For more information, see [Monitoring Amazon RDS log files \(p. 680\)](#).

You can also upload the upgrade logs to Amazon CloudWatch Logs. For more information, see [Publishing PostgreSQL logs to Amazon CloudWatch Logs \(p. 721\)](#).

- To verify that everything works as expected, test your application on the upgraded database with a similar workload. After the upgrade is verified, you can delete this test instance.

Automatic minor version upgrades for PostgreSQL

If you enable the **Auto minor version upgrade** option when creating or modifying a DB instance, you can have your DB instance automatically upgraded.

For each RDS for PostgreSQL major version, one minor version is designated by RDS as the automatic upgrade version. After a minor version has been tested and approved by Amazon RDS, the minor version upgrade occurs automatically during your maintenance window. RDS doesn't automatically set newer released minor versions as the automatic upgrade version. Before RDS designates a newer automatic upgrade version, several criteria are considered, such as the following:

- Known security issues
- Bugs in the PostgreSQL community version
- Overall fleet stability since the minor version was released

You can use the following AWS CLI command to determine the current automatic minor upgrade target version for a specified PostgreSQL minor version in a specific AWS Region.

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

For example, the following AWS CLI command determines the automatic minor upgrade target for PostgreSQL minor version 10.11 in the US East (Ohio) AWS Region (us-east-2).

For Linux, macOS, or Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version 10.11 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

For Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version 10.11 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Your output is similar to the following.

DescribeDBEngineVersions	
AutoUpgrade	EngineVersion
False	10.12
False	10.13
False	10.14
False	10.15
False	10.16
True	10.17
False	10.18

False	11.6
False	11.7
False	11.8
False	11.9
False	11.10
False	11.11
False	11.12
False	11.13

In this example, the AutoUpgrade value is True for PostgreSQL version 10.17. So, the automatic minor upgrade target is PostgreSQL version 10.17, which is highlighted in the output.

A PostgreSQL DB instance is automatically upgraded during your maintenance window if the following criteria are met:

- The DB instance has the **Auto minor version upgrade** option enabled.
- The DB instance is running a minor DB engine version that is less than the current automatic upgrade minor version.

For more information, see [Automatically upgrading the minor engine version \(p. 362\)](#).

Note

A PostgreSQL upgrade doesn't upgrade PostgreSQL extensions. To upgrade extensions, see [Upgrading PostgreSQL extensions \(p. 1849\)](#).

Upgrading PostgreSQL extensions

A PostgreSQL engine upgrade doesn't upgrade most PostgreSQL extensions. To update an extension after a version upgrade, use the `ALTER EXTENSION UPDATE` command.

Note

For information about updating the PostGIS extension, see [Managing spatial data with the PostGIS extension \(p. 1980\) \(Step 6: Upgrade the PostGIS extension \(p. 1983\)\)](#).

To update the `pg_repack` extension, drop the extension and then create the new version in the upgraded DB instance. For more information, see [pg_repack installation](#) in the `pg_repack` documentation.

To upgrade an extension, use the following command.

```
ALTER EXTENSION extension_name UPDATE TO 'new_version'
```

For the list of supported versions of PostgreSQL extensions, see [Supported PostgreSQL extension versions \(p. 1807\)](#).

To list your currently installed extensions, use the PostgreSQL `pg_extension` catalog in the following command.

```
SELECT * FROM pg_extension;
```

To view a list of the specific extension versions that are available for your installation, use the PostgreSQL `pg_available_extension_versions` view in the following command.

```
SELECT * FROM pg_available_extension_versions;
```

Upgrading a PostgreSQL DB snapshot engine version

With Amazon RDS, you can create a storage volume DB snapshot of your PostgreSQL DB instance. When you create a DB snapshot, the snapshot is based on the engine version used by your Amazon RDS instance. In addition to upgrading the DB engine version of your DB instance, you can also upgrade the engine version for your DB snapshots.

After restoring a DB snapshot upgraded to a new engine version, make sure to test that the upgrade was successful. For more information about a major version upgrade, see [Upgrading the PostgreSQL DB engine for Amazon RDS \(p. 1839\)](#). To learn how to restore a DB snapshot, see [Restoring from a DB snapshot \(p. 452\)](#).

You can upgrade manual DB snapshots that are either encrypted or not encrypted.

For the list of engine versions that are available for upgrading a DB snapshot, see [Upgrading the PostgreSQL DB engine for Amazon RDS](#).

Note

You can't upgrade automated DB snapshots that are created during the automated backup process.

Console

To upgrade a DB snapshot

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Snapshots**.
3. Choose the snapshot that you want to upgrade.
4. For **Actions**, choose **Upgrade snapshot**. The **Upgrade snapshot** page appears.
5. Choose the **New engine version** to upgrade to.
6. Choose **Save changes** to upgrade the snapshot.

During the upgrade process, all snapshot actions are disabled for this DB snapshot. Also, the DB snapshot status changes from **available** to **upgrading**, and then changes to **active** upon completion. If the DB snapshot can't be upgraded because of snapshot corruption issues, the status changes to **unavailable**. You can't recover the snapshot from this state.

Note

If the DB snapshot upgrade fails, the snapshot is rolled back to the original state with the original version.

AWS CLI

To upgrade a DB snapshot to a new database engine version, use the AWS CLI [modify-db-snapshot](#) command.

Parameters

- **--db-snapshot-identifier** – The identifier of the DB snapshot to upgrade. The identifier must be a unique Amazon Resource Name (ARN). For more information, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).
- **--engine-version** – The engine version to upgrade the DB snapshot to.

Example

For Linux, macOS, or Unix:

```
aws rds modify-db-snapshot \
--db-snapshot-identifier my_db_snapshot \
--engine-version new_version
```

For Windows:

```
aws rds modify-db-snapshot ^
--db-snapshot-identifier my_db_snapshot ^
--engine-version new_version
```

RDS API

To upgrade a DB snapshot to a new database engine version, call the Amazon RDS API [ModifyDBSnapshot](#) operation.

- **DBSnapshotIdentifier** – The identifier of the DB snapshot to upgrade. The identifier must be a unique Amazon Resource Name (ARN). For more information, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).
- **EngineVersion** – The engine version to upgrade the DB snapshot to.

Working with read replicas for Amazon RDS for PostgreSQL

You can scale reads for your Amazon RDS for PostgreSQL DB instance by adding read replicas to the instance. As with other Amazon RDS database engines, RDS for PostgreSQL uses the native replication mechanisms of PostgreSQL to keep read replicas up to date with changes on the source DB. For general information about read replicas and Amazon RDS, see [Working with read replicas \(p. 370\)](#).

Following, you can find information specific to working with read replicas with RDS for PostgreSQL.

Contents

- [Read replica limitations with PostgreSQL \(p. 1852\)](#)
- [Read replica configuration with PostgreSQL \(p. 1853\)](#)
 - [Using RDS for PostgreSQL read replicas with Multi-AZ configurations \(p. 1854\)](#)
 - [Using cascading read replicas with RDS for PostgreSQL \(p. 1854\)](#)
- [How streaming replication works for different RDS for PostgreSQL versions \(p. 1855\)](#)
 - [Understanding the parameters that control PostgreSQL replication \(p. 1856\)](#)
 - [Example: How a read replica recovers from replication interruptions \(p. 1857\)](#)
- [Monitoring and tuning the replication process \(p. 1857\)](#)
 - [Monitoring replication slots for your RDS for PostgreSQL DB instance \(p. 1858\)](#)

Read replica limitations with PostgreSQL

The following are limitations for PostgreSQL read replicas:

- PostgreSQL read replicas are read-only. Although a read replica isn't a writeable DB instance, you can promote it to become a standalone RDS for PostgreSQL DB instance. However, the process isn't reversible.
- You can't create a read replica from another read replica if your RDS for PostgreSQL DB instance is running a PostgreSQL version earlier than 14.1. RDS for PostgreSQL supports cascading read replicas on RDS for PostgreSQL version 14.1 and higher releases only. For more information, see [Using cascading read replicas with RDS for PostgreSQL \(p. 1854\)](#).
- If you promote a PostgreSQL read replica, it becomes a writable DB instance. It stops receiving write-ahead log (WAL) files from a source DB instance, and it's no longer a read-only instance. You can create new read replicas from the promoted DB instance as you do for any RDS for PostgreSQL DB instance. For more information, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).
- If you promote a PostgreSQL read replica from within a replication chain (a series of cascading read replicas), any existing downstream read replicas continue receiving WAL files from the promoted instance, automatically. For more information, see [Using cascading read replicas with RDS for PostgreSQL \(p. 1854\)](#).
- If no user transactions are running on the source DB instance, the associated PostgreSQL read replica reports a replication lag of up to five minutes. The replica lag is calculated as `currentTime - lastCommittedTransactionTimestamp`, which means that when no transactions are being processed, the value of replica lag increases for a period of time until the write-ahead log (WAL) segment switches. By default RDS for PostgreSQL switches the WAL segment every 5 minutes, which results in a transaction record and a decrease in the reported lag.
- You can't turn on automated backups for PostgreSQL read replicas for RDS for PostgreSQL versions earlier than 14.1. Automated backups for read replicas are supported for RDS for PostgreSQL 14.1 and higher versions only. For RDS for PostgreSQL 13 and earlier versions, create a snapshot from a read replica if you want a backup of it.

- Point-in-time recovery (PITR) isn't supported for read replicas. You can use PITR with a primary (writer) instance only, not a read replica. To learn more, see [Restoring a DB instance to a specified time \(p. 499\)](#).

Read replica configuration with PostgreSQL

RDS for PostgreSQL uses PostgreSQL native streaming replication to create a read-only copy of a source DB instance. This read replica DB instance is an asynchronously created physical replica of the source DB instance. It's created by a special connection that transmits write ahead log (WAL) data from the source DB instance to the read replica. For more information, see [Streaming Replication](#) in the PostgreSQL documentation.

PostgreSQL asynchronously streams database changes to this secure connection as they're made on the source DB instance. You can encrypt communications from your client applications to the source DB instance or any read replicas by setting the `ssl` parameter to 1. For more information, see [Using SSL with a PostgreSQL DB instance \(p. 1816\)](#).

PostgreSQL uses a *replication* role to perform streaming replication. The role is privileged, but you can't use it to modify any data. PostgreSQL uses a single process for handling replication.

You can create a PostgreSQL read replica without affecting operations or users of the source DB instance. Amazon RDS sets the necessary parameters and permissions for you, on the source DB instance and the read replica, without affecting the service. A snapshot is taken of the source DB instance, and this snapshot is used to create the read replica. If you delete the read replica at some point in the future, no outage occurs.

You can create up to 15 read replicas from one source DB instance within the same Region. As of RDS for PostgreSQL 14.1, you can also create up to three levels of read replica in a chain (cascade) from a source DB instance. For more information, see [Using cascading read replicas with RDS for PostgreSQL \(p. 1854\)](#). In all cases, the source DB instance needs to have automated backups configured. You do this by setting the backup retention period on your DB instance to any value other than 0. For more information, see [Creating a read replica \(p. 375\)](#).

You can create read replicas for your RDS for PostgreSQL DB instance in the same AWS Region as your source DB instance. This is known as *in-Region* replication. You can also create read replicas in different AWS Regions than the source DB instance. This is known as *cross-Region* replication. For more information about setting up cross-Region read replicas, see [Creating a read replica in a different AWS Region \(p. 383\)](#). The various mechanisms supporting the replication process for in-Region and cross-Region differ slightly depending on the RDS for PostgreSQL version as explained in [How streaming replication works for different RDS for PostgreSQL versions \(p. 1855\)](#).

For replication to operate effectively, each read replica should have the same amount of compute and storage resources as the source DB instance. If you scale the source DB instance, be sure to also scale the read replicas.

Amazon RDS overrides any incompatible parameters on a read replica if they prevent the read replica from starting. For example, suppose that the `max_connections` parameter value is higher on the source DB instance than on the read replica. In that case, Amazon RDS updates the parameter on the read replica to be the same value as that on the source DB instance.

RDS for PostgreSQL read replicas have access to external databases that are available through foreign data wrappers (FDWs) on the source DB instance. For example, suppose that your RDS for PostgreSQL DB instance is using the `mysql_fdw` wrapper to access data from RDS for MySQL. If so, your read replicas can also access that data. Other supported FDWs include `oracle_fdw`, `postgres_fdw`, and `tds_fdw`. For more information, see [Working with the supported foreign data wrappers for Amazon RDS for PostgreSQL \(p. 1987\)](#).

Using RDS for PostgreSQL read replicas with Multi-AZ configurations

You can create a read replica from a single-AZ or Multi-AZ DB instance. You can use Multi-AZ deployments to improve the durability and availability of critical data, with a standby replica. A *standby replica* is a dedicated read replica that can assume the workload if the source DB fails over. You can't use your standby replica to serve read traffic. However, you can create read replicas from high-traffic Multi-AZ DB instances to offload read-only queries. To learn more about Multi-AZ deployments, see [Multi-AZ DB instance deployments \(p. 122\)](#).

If the source DB instance of a Multi-AZ deployment fails over to a standby, the associated read replicas switch to using the standby (now primary) as their replication source. The read replicas might need to restart, depending on the RDS for PostgreSQL version, as follows:

- **PostgreSQL 13 and higher versions** – Restarting isn't required. The read replicas are automatically synchronized with the new primary. However, in some cases your client application might cache Domain Name Service (DNS) details for your read replicas. If so, set the time-to-live (TTL) value to less than 30 seconds. Doing this prevents the read replica from holding on to a stale IP address (and thus, prevents it from synchronizing with the new primary). To learn more about this and other best practices, see [Amazon RDS basic operational guidelines \(p. 216\)](#).
- **PostgreSQL 12 and all earlier versions** – The read replicas restart automatically after a fail over to the standby replica because the standby (now primary) has a different IP address and a different instance name. Restarting synchronizes the read replica with the new primary.

To learn more about failover, see [Failover process for Amazon RDS \(p. 123\)](#). To learn more about how read replicas work in a Multi-AZ deployment, see [Working with read replicas \(p. 370\)](#).

To provide failover support for a read replica, you can create the read replica as a Multi-AZ DB instance so that Amazon RDS creates a standby of your replica in another Availability Zone (AZ). Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance.

Using cascading read replicas with RDS for PostgreSQL

As of version 14.1, RDS for PostgreSQL supports cascading read replicas. With *cascading read replicas*, you can scale reads without adding overhead to your source RDS for PostgreSQL DB instance. Updates to the WAL log aren't sent by the source DB instance to each read replica. Instead, each read replica in a cascading series sends WAL log updates to the next read replica in the series. This reduces the burden on the source DB instance.

With cascading read replicas, your RDS for PostgreSQL DB instance sends WAL data to the first read replica in the chain. That read replica then sends WAL data to the second replica in the chain, and so on. The end result is that all read replicas in the chain have the changes from the RDS for PostgreSQL DB instance, but without the overhead solely on the source DB instance.

You can create a series of up to three read replicas in a chain from a source RDS for PostgreSQL DB instance. For example, suppose that you have an RDS for PostgreSQL 14.1 DB instance, `rpg-db-main`. You can do the following:

- Starting with `rpg-db-main`, create the first read replica in the chain, `read-replica-1`.
- Next, from `read-replica-1`, create the next read replica in the chain, `read-replica-2`.
- Finally, from `read-replica-2`, create the third read replica in the chain, `read-replica-3`.

You can't create another read replica beyond this third cascading read replica in the series for `rpg-db-main`. A complete series of instances from an RDS for PostgreSQL source DB instance through to the end of a series of cascading read replicas can consist of at most four DB instances.

For cascading read replicas to work, turn on automatic backups on your RDS for PostgreSQL. Create the read replica first and then turn on automatic backups on the RDS for PostgreSQL DB instance. The process is the same as for other Amazon RDS DB engines. For more information, see [Creating a read replica \(p. 375\)](#).

As with any read replica, you can promote a read replica that's part of a cascade. Promoting a read replica from within a chain of read replicas removes that replica from the chain. For example, suppose that you want to move some of the workload off of your `rpg-db-main` DB instance to a new instance for use by the accounting department only. Assuming the chain of three read replicas from the example, you decide to promote `read-replica-2`. The chain is affected as follows:

- Promoting `read-replica-2` removes it from the replication chain.
 - It is now a full read/write DB instance.
 - It continues replicating to `read-replica-3`, just as it was doing before promotion.
- Your `rpg-db-main` continues replicating to `read-replica-1`.

For more information about promoting read replicas, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).

Note

For cascading read replicas, RDS for PostgreSQL supports 15 read replicas for each source DB instance at first level of replication, and 5 read replicas for each source DB instance at the second and third level of replication.

How streaming replication works for different RDS for PostgreSQL versions

As discussed in [Read replica configuration with PostgreSQL \(p. 1853\)](#), RDS for PostgreSQL uses PostgreSQL's native streaming replication protocol to send WAL data from the source DB instance. It sends source WAL data to read replicas for both in-Region and cross-Region read replicas. With version 9.4, PostgreSQL introduced physical replication slots as a supporting mechanism for the replication process.

A *physical replication slot* prevents a source DB instance from removing WAL data before it's consumed by all read replicas. Each read replica has its own physical slot on the source DB instance. The slot keeps track of the oldest WAL (by logical sequence number, LSN) that might be needed by the replica. After all slots and DB connections have progressed beyond a given WAL (LSN), that LSN becomes a candidate for removal at the next checkpoint.

Amazon RDS uses Amazon S3 to archive WAL data. For in-Region read replicas, you can use this archived data to recover the read replica when necessary. An example of when you might do so is if the connection between source DB and read replica is interrupted for any reason.

In the following table, you can find a summary of differences between PostgreSQL versions and the supporting mechanisms for in-Region and cross-Region used by RDS for PostgreSQL.

In-Region	Cross-Region
PostgreSQL 14.1 and higher versions <ul style="list-style-type: none">• Replication slots• Amazon S3 archive	<ul style="list-style-type: none">• Replication slots

In-Region	Cross-Region
PostgreSQL 13 and lower versions	
• Amazon S3 archive	• Replication slots

For more information, see [Monitoring and tuning the replication process \(p. 1857\)](#).

Understanding the parameters that control PostgreSQL replication

The following parameters affect the replication process and determine how well read replicas stay up to date with the source DB instance:

max_wal_senders

The `max_wal_senders` parameter specifies the maximum number of connections that the source DB instance can support at the same time over the streaming replication protocol. The default for RDS for PostgreSQL 13 and higher releases is 20. This parameter should be set to slightly higher than the actual number of read replicas. If this parameter is set too low for the number of read replicas, replication stops.

For more information, see [max_wal_senders](#) in the PostgreSQL documentation.

wal_keep_segments

The `wal_keep_segments` parameter specifies the number of write-ahead log (WAL) files that the source DB instance keeps in the `pg_wal` directory. The default setting is 32.

If `wal_keep_segments` isn't set to a large enough value for your deployment, a read replica can fall so far behind that streaming replication stops. If that happens, Amazon RDS generates a replication error and begins recovery on the read replica. It does so by replaying the source DB instance's archived WAL data from Amazon S3. This recovery process continues until the read replica has caught up enough to continue streaming replication. You can see this process in action as captured by the PostgreSQL log in [Example: How a read replica recovers from replication interruptions \(p. 1857\)](#).

Note

In PostgreSQL version 13, the `wal_keep_segments` parameter is named `wal_keep_size`. It serves the same purpose as `wal_keep_segments`, but its default value is in megabytes (MB) (2048 MB) rather than the number of files. For more information, see [wal_keep_segments](#) and [wal_keep_size](#) in the PostgreSQL documentation.

max_slot_wal_keep_size

The `max_slot_wal_keep_size` parameter controls the quantity of WAL data that the RDS for PostgreSQL DB instance retains in the `pg_wal` directory to serve slots. This parameter is used for configurations that use replication slots. The default value for this parameter is -1, meaning that there's no limit to how much WAL data is kept on the source DB instance. For information about monitoring your replication slots, see [Monitoring replication slots for your RDS for PostgreSQL DB instance \(p. 1858\)](#).

For more information about this parameter, see [max_slot_wal_keep_size](#) in the PostgreSQL documentation.

Whenever the stream that provides WAL data to a read replica is interrupted, PostgreSQL switches into recovery mode. It restores the read replica by using archived WAL data from Amazon S3 or by using

the using WAL data associated with the replication slot. When this process is complete, PostgreSQL re-establishes streaming replication.

Example: How a read replica recovers from replication interruptions

In the following example, you find the log details that demonstrate the recovery process for a read replica. The example is from an RDS for PostgreSQL DB instance running PostgreSQL version 12.9 in the same AWS Region as the source DB, so replication slots aren't used. The recovery process is the same for other RDS for PostgreSQL DB instances running PostgreSQL earlier than version 14.1 with in-Region read replicas.

When the read replica lost contact with the source DB instance, Amazon RDS records the issue in the log as **FATAL: could not receive data from WAL stream** message, along with the **ERROR: requested WAL segment ... has already been removed**. As shown in the bold line, Amazon RDS recovers the replica by replaying an archived WAL file.

```
2014-11-07 19:01:10 UTC::@:[23180]:DEBUG: switched WAL source from archive to stream after failure
2014-11-07 19:01:10 UTC::@:[11575]:LOG: started streaming WAL from primary at 1A/D3000000
on timeline 1
2014-11-07 19:01:10 UTC::@:[11575]:FATAL: could not receive data from WAL stream:
ERROR: requested WAL segment 000000010000001A000000D3 has already been removed
2014-11-07 19:01:10 UTC::@:[23180]:DEBUG: could not restore file "00000002.history" from
archive: return code 0
2014-11-07 19:01:15 UTC::@:[23180]:DEBUG: switched WAL source from stream to archive after
failure recovering 000000010000001A000000D3
2014-11-07 19:01:16 UTC::@:[23180]:LOG: restored log file "000000010000001A000000D3" from
archive
```

When Amazon RDS replays enough archived WAL data on the replica to catch up, streaming to the read replica begins again. When streaming resumes, Amazon RDS writes an entry to the log file similar to the following.

```
2014-11-07 19:41:36 UTC::@:[24714]:LOG:started streaming WAL from primary at 1B/B6000000 on
timeline 1
```

Monitoring and tuning the replication process

We strongly recommend that you routinely monitor your RDS for PostgreSQL DB instance and read replicas. You need to ensure that your read replicas are keeping up with changes on the source DB instance. Amazon RDS transparently recovers your read replicas when interruptions to the replication process occur. However, it's best to avoid needing to recover at all. Recovering using replication slots is faster than using the Amazon S3 archive, but any recovery process can affect read performance.

To determine how well your read replicas are keeping up with the source DB instance, you can do the following:

- **Check the amount of ReplicaLag between source DB instance and replicas.** *Replica lag* is the amount of time, in milliseconds, that a read replica lags behind its source DB instance. This metric reports the result of the following query.

```
SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS replica_lag
```

Replica lag is an indication of how well a read replica is keeping up with the source DB instance. It's the amount of latency between the source DB instance and a specific read instance. A high value for replica lag can indicate a mismatch between the DB instance classes or storage types (or both) used by the source DB instance and its read replicas. The DB instance class and storage types for DB source instance and all read replicas should be the same.

Replica lag can also be the result of intermittent connection issues. You can monitor replication lag in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric. To learn more about ReplicaLag and other metrics for Amazon RDS, see [Amazon CloudWatch metrics for Amazon RDS \(p. 609\)](#).

- **Check the PostgreSQL log for information you can use to adjust your settings.** At every checkpoint, the PostgreSQL log captures the number of recycled transaction log files, as shown in the following example.

```
2014-11-07 19:59:35 UTC::@:[26820]:LOG:  checkpoint complete: wrote 376 buffers (0.2%);  
0 transaction log file(s) added, 0 removed, 1 recycled; write=35.681 s, sync=0.013 s,  
total=35.703 s;  
sync files=10, longest=0.013 s, average=0.001 s
```

You can use this information to figure out how many transaction files are being recycled in a given time period. You can then change the setting for wal_keep_segments if necessary. For example, suppose that the PostgreSQL log at checkpoint complete shows 35 recycled for a 5-minute interval. In this case, the wal_keep_segments default value of 32 isn't sufficient to keep pace with the streaming activity, so you should increase the value of this parameter.

- **Use Amazon CloudWatch to monitor metrics that can predict replication issues.** Rather than analyzing the PostgreSQL log directly, you can use Amazon CloudWatch to check metrics that have been collected. For example, you can check the value of the TransactionLogsGeneration metric to see how much WAL data is being generated by the source DB instance. In some cases, the workload on your DB instance might generate a large amount of WAL data. If so, you might need to change the DB instance class for your source DB instance and read replicas. Using an instance class with high (10 Gbps) network performance can reduce replica lag.

Monitoring replication slots for your RDS for PostgreSQL DB instance

All versions of RDS for PostgreSQL use replication slots for cross-Region read replicas. RDS for PostgreSQL 14.1 and higher versions use replication slots for in-Region read replicas. In-region read replicas also use Amazon S3 to archive WAL data. In other words, if your DB instance and read replicas are running PostgreSQL 14.1 or higher, replication slots and Amazon S3 archives are both available for recovering the read replica. Recovering a read replica using its replication slot is faster than recovering from Amazon S3 archive. So, we recommend that you monitor the replication slots and related metrics.

You can view the replication slots on your RDS for PostgreSQL DB instances by querying the pg_replication_slots view, as follows.

```
postgres=> SELECT * FROM pg_replication_slots;
slot_name           | plugin | slot_type | datoid | database | temporary | active
| active_pid | xmin | catalog_xmin | restart_lsn | confirmed_flush_lsn | wal_status | safe_wal_size | two_phase
-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+-----+-----+
rds_us_west_1_db_5555555555 |      | physical |      |      | f | reserved | t
13194 |      | 23/D8000060 |      |      | f | reserved | t
(1 row)
```

The wal_status of reserved value means that the amount of WAL data held by the slot is within the bounds of the max_wal_size parameter. In other words, the replication slot is properly sized. Other possible status values are as follows:

- **extended** – The slot exceeds the `max_wal_size` setting, but the WAL data is retained.
- **unreserved** – The slot no longer has the all required WAL data. Some of it will be removed at the next checkpoint.
- **lost** – Some required WAL data has been removed. The slot is no longer usable.

The `pg_replication_slots` view shows you the current state of your replication slots. To assess the performance of your replication slots, you can use Amazon CloudWatch and monitor the following metrics:

- **OldestReplicationSlotLag** – Lists the slot that has the most lag, that is the one that's furthest behind the primary. This lag can be associated with the read replica but also the connection.
- **TransactionLogsDiskUsage** – Shows how much storage is being used for WAL data. When a read replica lags significantly, the value of this metric can increase substantially.

To learn more about using Amazon CloudWatch and its metrics for RDS for PostgreSQL, see [Monitoring Amazon RDS metrics with Amazon CloudWatch \(p. 528\)](#). For more information about monitoring streaming replication on your RDS for PostgreSQL DB instances, see [Best practices for Amazon RDS PostgreSQL replication](#) on the [AWS Database Blog](#).

Importing data into PostgreSQL on Amazon RDS

Suppose that you have an existing PostgreSQL deployment that you want to move to Amazon RDS. The complexity of your task depends on the size of your database and the types of database objects that you're transferring. For example, consider a database that contains datasets on the order of gigabytes, along with stored procedures and triggers. Such a database is going to be more complicated than a simple database with only a few megabytes of test data and no triggers or stored procedures.

We recommend that you use native PostgreSQL database migration tools under the following conditions:

- You have a homogeneous migration, where you are migrating from a database with the same database engine as the target database.
- You are migrating an entire database.
- The native tools allow you to migrate your system with minimal downtime.

In most other cases, performing a database migration using AWS Database Migration Service (AWS DMS) is the best approach. AWS DMS can migrate databases without downtime and, for many database engines, continue ongoing replication until you are ready to switch over to the target database. You can migrate to either the same database engine or a different database engine using AWS DMS. If you are migrating to a different database engine than your source database, you can use the AWS Schema Conversion Tool (AWS SCT). You use AWS SCT to migrate schema objects that are not migrated by AWS DMS. For more information about AWS DMS, see [What is AWS Database Migration Service?](#)

Modify your DB parameter group to include the following settings *for your import only*. You should test the parameter settings to find the most efficient settings for your DB instance size. You also need to revert back to production values for these parameters after your import completes.

Modify your DB instance settings to the following:

- Disable DB instance backups (set backup_retention to 0).
- Disable Multi-AZ.

Modify your DB parameter group to include the following settings. You should only use these settings when importing data. You should test the parameter settings to find the most efficient settings for your DB instance size. You also need to revert back to production values for these parameters after your import completes.

Parameter	Recommended value when importing	Description
maintenance_work_mem	524288, 1048576, 2097152, or 4194304 (in KB). These settings are comparable to 512 MB, 1 GB, 2 GB, and 4 GB.	The value for this setting depends on the size of your host. This parameter is used during CREATE INDEX statements and each parallel command can use this much memory. Calculate the best value so that you don't set this value so high that you run out of memory.
max_wal_size	256 (for version 9.6), 4096 (for versions 10 and higher)	Maximum size to let the WAL grow during automatic checkpoints. Increasing this parameter can increase the amount of time needed for crash recovery. This parameter replaces checkpoint_segments for PostgreSQL 9.6 and later.

Parameter	Recommended value when importing	Description
		For PostgreSQL version 9.6, this value is in 16 MB units. For later versions, the value is in 1 MB units. For example, in version 9.6, 128 means 128 chunks that are each 16 MB in size. In version 12.4, 2048 means 2048 chunks that are each 1 MB in size.
checkpoint_timeout	1800	The value for this setting allows for less frequent WAL rotation.
synchronous_commit	Off	Disable this setting to speed up writes. Turning this parameter off can increase the risk of data loss in the event of a server crash (do not turn off FSYNC).
wal_buffers	8192	This value is in 8 KB units. This again helps your WAL generation speed
autovacuum	Off	Disable the PostgreSQL auto vacuum parameter while you are loading data so that it doesn't use resources

Use the `pg_dump -Fc` (compressed) or `pg_restore -j` (parallel) commands with these settings.

Note

The PostgreSQL command `pg_dumpall` requires `super_user` permissions that are not granted when you create a DB instance, so it cannot be used for importing data.

Topics

- [Importing a PostgreSQL database from an Amazon EC2 instance \(p. 1861\)](#)
- [Using the \copy command to import data to a table on a PostgreSQL DB instance \(p. 1863\)](#)
- [Importing data from Amazon S3 into an RDS for PostgreSQL DB instance \(p. 1864\)](#)
- [Transporting PostgreSQL databases between DB instances \(p. 1877\)](#)

Importing a PostgreSQL database from an Amazon EC2 instance

If you have data in a PostgreSQL server on an Amazon EC2 instance and want to move it to a PostgreSQL DB instance, you can use the following process. The following list shows the steps to take. Each step is discussed in more detail in the following sections.

1. Create a file using `pg_dump` that contains the data to be loaded
2. Create the target DB instance
3. Use `psql` to create the database on the DB instance and load the data
4. Create a DB snapshot of the DB instance

Step 1: Create a file using pg_dump that contains the data to load

The pg_dump utility uses the COPY command to create a schema and data dump of a PostgreSQL database. The dump script generated by pg_dump loads data into a database with the same name and recreates the tables, indexes, and foreign keys. You can use the pg_restore command and the -d parameter to restore the data to a database with a different name.

Before you create the data dump, you should query the tables to be dumped to get a row count so you can confirm the count on the target DB instance.

The following command creates a dump file called mydb2dump.sql for a database called mydb2.

```
prompt>pg_dump dbname=mydb2 -f mydb2dump.sql
```

Step 2: Create the target DB instance

Create the target PostgreSQL DB instance using either the Amazon RDS console, AWS CLI, or API. Create the instance with the backup retention setting set to 0 and disable Multi-AZ. Doing so allows faster data import. You must create a database on the instance before you can dump the data. The database can have the same name as the database that is contained the dumped data. Alternatively, you can create a database with a different name. In this case, you use the pg_restore command and the -d parameter to restore the data into the newly named database.

For example, the following commands can be used to dump, restore, and rename a database.

```
pg_dump -Fc -v -h [endpoint of instance] -U [master username] [database] > [database].dump
createdb [new database name]
pg_restore -v -h [endpoint of instance] -U [master username] -d [new database
name] [database].dump
```

Step 3: Use psql to create the database on the DB instance and load data

You can use the same connection you used to run the pg_dump command to connect to the target DB instance and recreate the database. Using *psql*, you can use the master user name and master password to create the database on the DB instance

The following example uses *psql* and a dump file named mydb2dump.sql to create a database called mydb2 on a PostgreSQL DB instance called mypginstance:

For Linux, macOS, or Unix:

```
psql \
-f mydb2dump.sql \
--host mypginstance.55555555555.aws-region.rds.amazonaws.com \
--port 8199 \
--username myawsuser \
--password password \
--dbname mydb2
```

For Windows:

```
psql ^
-f mydb2dump.sql ^
```

```
--host mypginstance.55555555555.aws-region.rds.amazonaws.com ^
--port 8199 ^
--username myawsuser ^
--password password ^
--dbname mydb2
```

Step 4: Create a DB snapshot of the DB instance

Once you have verified that the data was loaded into your DB instance, we recommend that you create a DB snapshot of the target PostgreSQL DB instance. DB snapshots are complete backups of your DB instance that can be used to restore your DB instance to a known state. A DB snapshot taken immediately after the load protects you from having to load the data again in case of a mishap. You can also use such a snapshot to seed new DB instances. For information about creating a DB snapshot, see [Creating a DB snapshot \(p. 448\)](#).

Using the \copy command to import data to a table on a PostgreSQL DB instance

The PostgreSQL \copy command is a meta-command available from the psql interactive client tool. You can use \copy to import data into a table on your RDS for PostgreSQL DB instance. To use the \copy command, you need to first create the table structure on the target DB instance so that \copy has a destination for the data being copied.

You can use \copy to load data from a comma-separated values (CSV) file, such as one that's been exported and saved to your client workstation.

To import the CSV data to the target RDS for PostgreSQL DB instance, first connect to the target DB instance using psql.

```
psql --host=db-instance.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=target-db
```

You then run \copy command with the following parameters to identify the target for the data and its format.

- **target_table** – The name of the table that should receive the data being copied from the CSV file.
- **column_list** – Column specifications for the table.
- '**filename**' – The complete path to the CSV file on your local workstation.

```
\copy target_table from '/path/to/local/filename.csv' WITH DELIMITER ',' CSV;
```

If your CSV file has column heading information, you can use this version of the command and parameters.

```
\copy target_table (column-1, column-2, column-3, ...)
from '/path/to/local/filename.csv' WITH DELIMITER ',' CSV HEADER;
```

If the \copy command fails, PostgreSQL outputs error messages.

You can also combine the psql command with the \copy meta-command as shown in the following examples. This example uses *source-table* as the source table name, *source-table.csv* as the .csv file, and *target-db* as the target database:

For Linux, macOS, or Unix:

```
$psql target-db \
-U <admin user> \
-p <port> \
-h <DB instance name> \
-c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

For Windows:

```
$psql target-db ^
-U <admin user> ^
-p <port> ^
-h <DB instance name> ^
-c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

For complete details about the \copy command, see the [psql](#) page in the PostgreSQL documentation, in the *Meta-Commands* section.

Importing data from Amazon S3 into an RDS for PostgreSQL DB instance

You can import data that's been stored using Amazon Simple Storage Service into a table on an RDS for PostgreSQL DB instance. To do this, you first install the RDS for PostgreSQL aws_s3 extension. This extension provides the functions that you use to import data from an Amazon S3 bucket. A *bucket* is an Amazon S3 container for objects and files. The data can be in a comma-separate value (CSV) file, a text file, or a compressed (gzip) file. Following, you can learn how to install the extension and how to import data from Amazon S3 into a table.

Your database must be running PostgreSQL version 10.7 or higher to import from Amazon S3 into RDS for PostgreSQL.

If you don't have data stored on Amazon S3, you need to first create a bucket and store the data. For more information, see the following topics in the *Amazon Simple Storage Service User Guide*.

- [Create a bucket](#)
- [Add an object to a bucket](#)

Note

Importing data from Amazon S3 isn't supported for Aurora Serverless v1. It is supported for Aurora Serverless v2.

Topics

- [Installing the aws_s3 extension \(p. 1864\)](#)
- [Overview of importing data from Amazon S3 data \(p. 1865\)](#)
- [Setting up access to an Amazon S3 bucket \(p. 1866\)](#)
- [Importing data from Amazon S3 to your RDS for PostgreSQL DB instance \(p. 1871\)](#)
- [Function reference \(p. 1873\)](#)

Installing the aws_s3 extension

Before you can use Amazon S3 with your RDS for PostgreSQL DB instance, you need to install the aws_s3 extension. This extension provides functions for importing data from an Amazon S3. It also provides functions for exporting data from an RDS for PostgreSQL DB instance to an Amazon S3

bucket. For more information, see [Exporting data from an RDS for PostgreSQL DB instance to Amazon S3 \(p. 1883\)](#). The `aws_s3` extension depends on some of the helper functions in the `aws_commons` extension, which is installed automatically when needed.

To install the `aws_s3` extension

1. Use `psql` (or `pgAdmin`) to connect to the RDS for PostgreSQL DB instance as a user that has `rds_superuser` privileges. If you kept the default name during the setup process, you connect as `postgres`.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres  
--password
```

2. To install the extension, run the following command.

```
postgres=> CREATE EXTENSION aws_s3 CASCADE;  
NOTICE: installing required extension "aws_commons"  
CREATE EXTENSION
```

3. To verify that the extension is installed, you can use the `\dx` metacommand.

```
postgres=> \dx  
      List of installed extensions  
 Name | Version | Schema | Description  
-----+-----+-----+-----  
 aws_commons | 1.2 | public | Common data types across AWS services  
 aws_s3 | 1.1 | public | AWS S3 extension for importing data from S3  
 plpgsql | 1.0 | pg_catalog | PL/pgSQL procedural language  
(3 rows)
```

The functions for importing data from Amazon S3 and exporting data to Amazon S3 are now available to use.

Overview of importing data from Amazon S3 data

To import S3 data into Amazon RDS

First, gather the details that you need to supply to the function. These include the name of the table on your RDS for PostgreSQL DB instance, and the bucket name, file path, file type, and AWS Region where the Amazon S3 data is stored. For more information, see [View an object](#) in the *Amazon Simple Storage Service User Guide*.

1. Get the name of the table into which the `aws_s3.table_import_from_s3` function is to import the data. As an example, the following command creates a table `t1` that can be used in later steps.

```
postgres=> CREATE TABLE t1  
(col1 varchar(80),  
 col2 varchar(80),  
 col3 varchar(80));
```

2. Get the details about the Amazon S3 bucket and the data to import. To do this, open the Amazon S3 console at <https://console.aws.amazon.com/s3/>, and choose **Buckets**. Find the bucket containing your data in the list. Choose the bucket, open its Object overview page, and then choose Properties.

Make a note of the bucket name, path, the AWS Region, and file type. You need the Amazon Resource Name (ARN) later, to set up access to Amazon S3 through an IAM role. For more information, see [Setting up access to an Amazon S3 bucket \(p. 1866\)](#). The image following shows an example.

3. You can verify the path to the data on the Amazon S3 bucket by using the AWS CLI command `aws s3 cp`. If the information is correct, this command downloads a copy of the Amazon S3 file.

```
aws s3 cp s3://sample_s3_bucket/sample_file_path ./
```

4. Set up permissions on your RDS for PostgreSQL DB instance to allow access to the file on the Amazon S3 bucket. To do so, you use either an AWS Identity and Access Management (IAM) role or security credentials. For more information, see [Setting up access to an Amazon S3 bucket \(p. 1866\)](#).
5. Supply the path and other Amazon S3 object details gathered (see step 2) to the `create_s3_uri` function to construct an Amazon S3 URI object. To learn more about this function, see [aws_commons.create_s3_uri \(p. 1876\)](#). The following is an example of constructing this object during a `psql` session.

```
postgres=> SELECT aws_commons.create_s3_uri(
    'docs-lab-store-for-rpg',
    'versions_and_jdks_listing.csv',
    'us-west-1'
) AS s3_uri \gset
```

In the next step, you pass this object (`aws_commons._s3_uri_1`) to the `aws_s3.table_import_from_s3` function to import the data to the table.

6. Invoke the `aws_s3.table_import_from_s3` function to import the data from Amazon S3 into your table. For reference information, see [aws_s3.table_import_from_s3 \(p. 1873\)](#). For examples, see [Importing data from Amazon S3 to your RDS for PostgreSQL DB instance \(p. 1871\)](#).

Setting up access to an Amazon S3 bucket

To import data from an Amazon S3 file, give the RDS for PostgreSQL DB instance permission to access the Amazon S3 bucket containing the file. You provide access to an Amazon S3 bucket in one of two ways, as described in the following topics.

Topics

- [Using an IAM role to access an Amazon S3 bucket \(p. 1867\)](#)

- [Using security credentials to access an Amazon S3 bucket \(p. 1870\)](#)
- [Troubleshooting access to Amazon S3 \(p. 1871\)](#)

Using an IAM role to access an Amazon S3 bucket

Before you load data from an Amazon S3 file, give your RDS for PostgreSQL DB instance permission to access the Amazon S3 bucket the file is in. This way, you don't have to manage additional credential information or provide it in the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function call.

To do this, create an IAM policy that provides access to the Amazon S3 bucket. Create an IAM role and attach the policy to the role. Then assign the IAM role to your DB instance.

Note

You can't associate an IAM role with an Aurora Serverless v1 DB cluster, so the following steps don't apply.

To give an RDS for PostgreSQL DB instance access to Amazon S3 through an IAM role

1. Create an IAM policy.

This policy provides the bucket and object permissions that allow your RDS for PostgreSQL DB instance to access Amazon S3.

Include in the policy the following required actions to allow the transfer of files from an Amazon S3 bucket to Amazon RDS:

- s3:GetObject
- s3>ListBucket

Include in the policy the following resources to identify the Amazon S3 bucket and objects in the bucket. This shows the Amazon Resource Name (ARN) format for accessing Amazon S3.

- arn:aws:s3:::*your-s3-bucket*
- arn:aws:s3:::*your-s3-bucket*/*

For more information on creating an IAM policy for RDS for PostgreSQL, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#). See also [Tutorial: Create and attach your first customer managed policy](#) in the *IAM User Guide*.

The following AWS CLI command creates an IAM policy named rds-s3-import-policy with these options. It grants access to a bucket named *your-s3-bucket*.

Note

Make a note of the Amazon Resource Name (ARN) of the policy returned by this command. You need the ARN in a subsequent step when you attach the policy to an IAM role.

Example

For Linux, macOS, or Unix:

```
aws iam create-policy \
--policy-name rds-s3-import-policy \
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
```

```
"s3:GetObject",
"s3>ListBucket"
],
"Effect": "Allow",
"Resource": [
    "arn:aws:s3:::your-s3-bucket",
    "arn:aws:s3:::your-s3-bucket/*"
]
}
]'
```

For Windows:

```
aws iam create-policy ^
--policy-name rds-s3-import-policy ^
--policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3>ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::your-s3-bucket",
                "arn:aws:s3:::your-s3-bucket/*"
            ]
        }
    ]
}'
```

2. Create an IAM role.

You do this so Amazon RDS can assume this IAM role to access your Amazon S3 buckets. For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based policies to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

If you use both global condition context keys and the `aws:SourceArn` value contains the account ID, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the policy, be sure to use the `aws:SourceArn` global condition context key with the full ARN of the resource. The following example shows how to do so using the AWS CLI command to create a role named `rds-s3-import-role`.

Example

For Linux, macOS, or Unix:

```
aws iam create-role \
```

```
--role-name rds-s3-import-role \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
            }
        ]
    }
}'
```

For Windows:

```
aws iam create-role ^
--role-name rds-s3-import-role ^
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
            }
        ]
    }
}'
```

3. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created in the previous step to the role named `rds-s3-import-role`. Replace `your-policy-arn` with the policy ARN that you noted in an earlier step.

Example

For Linux, macOS, or Unix:

```
aws iam attach-role-policy \
--policy-arn your-policy-arn \
--role-name rds-s3-import-role
```

For Windows:

```
aws iam attach-role-policy ^
--policy-arn your-policy-arn ^
```

```
--role-name rds-s3-import-role
```

4. Add the IAM role to the DB instance.

You do so by using the AWS Management Console or AWS CLI, as described following.

Console

To add an IAM role for a PostgreSQL DB instance using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose the PostgreSQL DB instance name to display its details.
3. On the **Connectivity & security** tab, in the **Manage IAM roles** section, choose the role to add under **Add IAM roles to this instance**.
4. Under **Feature**, choose **s3Import**.
5. Choose **Add role**.

AWS CLI

To add an IAM role for a PostgreSQL DB instance using the CLI

- Use the following command to add the role to the PostgreSQL DB instance named *my-db-instance*. Replace *your-role-arn* with the role ARN that you noted in a previous step. Use *s3Import* for the value of the --feature-name option.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-instance \  
  --db-instance-identifier my-db-instance \  
  --feature-name s3Import \  
  --role-arn your-role-arn \  
  --region your-region
```

For Windows:

```
aws rds add-role-to-db-instance ^  
  --db-instance-identifier my-db-instance ^  
  --feature-name s3Import ^  
  --role-arn your-role-arn ^  
  --region your-region
```

RDS API

To add an IAM role for a PostgreSQL DB instance using the Amazon RDS API, call the [AddRoleToDBInstance](#) operation.

Using security credentials to access an Amazon S3 bucket

If you prefer, you can use security credentials to provide access to an Amazon S3 bucket instead of providing access with an IAM role. You do so by specifying the `credentials` parameter in the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function call.

The `credentials` parameter is a structure of type `aws_commons._aws_credentials_1`, which contains AWS credentials. Use the [aws_commons.create_aws_credentials \(p. 1876\)](#) function to set the access key and secret key in an `aws_commons._aws_credentials_1` structure, as shown following.

```
postgres=> SELECT aws_commons.create_aws_credentials(
    'sample_access_key', 'sample_secret_key', '')
AS creds \gset
```

After creating the `aws_commons._aws_credentials_1` structure, use the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function with the `credentials` parameter to import the data, as shown following.

```
postgres=> SELECT aws_s3.table_import_from_s3(
    't', '', '(format csv)',
    :'s3_uri',
    :'creds'
);
```

Or you can include the [aws_commons.create_aws_credentials \(p. 1876\)](#) function call inline within the `aws_s3.table_import_from_s3` function call.

```
postgres=> SELECT aws_s3.table_import_from_s3(
    't', '', '(format csv)',
    :'s3_uri',
    aws_commons.create_aws_credentials('sample_access_key', 'sample_secret_key', '')
);
```

Troubleshooting access to Amazon S3

If you encounter connection problems when attempting to import data from Amazon S3, see the following for recommendations:

- [Troubleshooting Amazon RDS identity and access \(p. 2075\)](#)
- [Troubleshooting Amazon S3 in the Amazon Simple Storage Service User Guide](#)
- [Troubleshooting Amazon S3 and IAM in the IAM User Guide](#)

Importing data from Amazon S3 to your RDS for PostgreSQL DB instance

You import data from your Amazon S3 bucket by using the `table_import_from_s3` function of the `aws_s3` extension. For reference information, see [aws_s3.table_import_from_s3 \(p. 1873\)](#).

Note

The following examples use the IAM role method to allow access to the Amazon S3 bucket. Thus, the `aws_s3.table_import_from_s3` function calls don't include credential parameters.

The following shows a typical example.

```
postgres=> SELECT aws_s3.table_import_from_s3(
    't1',
    '',
    '(format csv)',
    :'s3_uri'
);
```

The parameters are the following:

- `t1` – The name for the table in the PostgreSQL DB instance to copy the data into.
- `''` – An optional list of columns in the database table. You can use this parameter to indicate which columns of the S3 data go in which table columns. If no columns are specified, all the columns are copied to the table. For an example of using a column list, see [Importing an Amazon S3 file that uses a custom delimiter \(p. 1872\)](#).
- `(format csv)` – PostgreSQL COPY arguments. The copy process uses the arguments and format of the [PostgreSQL COPY](#) command to import the data. Choices for format include comma-separated value (CSV) as shown in this example, text, and binary. The default is text.
- `s3_uri` – A structure that contains the information identifying the Amazon S3 file. For an example of using the `aws_commons.create_s3_uri (p. 1876)` function to create an `s3_uri` structure, see [Overview of importing data from Amazon S3 data \(p. 1865\)](#).

For more information about this function, see [aws_s3.table_import_from_s3 \(p. 1873\)](#).

The `aws_s3.table_import_from_s3` function returns text. To specify other kinds of files for import from an Amazon S3 bucket, see one of the following examples.

Topics

- [Importing an Amazon S3 file that uses a custom delimiter \(p. 1872\)](#)
- [Importing an Amazon S3 compressed \(gzip\) file \(p. 1873\)](#)
- [Importing an encoded Amazon S3 file \(p. 1873\)](#)

Importing an Amazon S3 file that uses a custom delimiter

The following example shows how to import a file that uses a custom delimiter. It also shows how to control where to put the data in the database table using the `column_list` parameter of the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function.

For this example, assume that the following information is organized into pipe-delimited columns in the Amazon S3 file.

```
1|foo1|bar1|elephant1
2|foo2|bar2|elephant2
3|foo3|bar3|elephant3
4|foo4|bar4|elephant4
...
```

To import a file that uses a custom delimiter

1. Create a table in the database for the imported data.

```
postgres=> CREATE TABLE test (a text, b text, c text, d text, e text);
```

2. Use the following form of the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function to import data from the Amazon S3 file.

You can include the `aws_commons.create_s3_uri (p. 1876)` function call inline within the `aws_s3.table_import_from_s3` function call to specify the file.

```
postgres=> SELECT aws_s3.table_import_from_s3(
    'test',
    'a,b,d,e',
    'DELIMITER ''|''',
    aws_commons.create_s3_uri('sampleBucket', 'pipeDelimitedSampleFile', 'us-east-2')
);
```

The data is now in the table in the following columns.

```
postgres=> SELECT * FROM test;
a | b | c | d | e
---+---+---+---+---+
1 | foo1 | | bar1 | elephant1
2 | foo2 | | bar2 | elephant2
3 | foo3 | | bar3 | elephant3
4 | foo4 | | bar4 | elephant4
```

Importing an Amazon S3 compressed (gzip) file

The following example shows how to import a file from Amazon S3 that is compressed with gzip. The file that you import needs to have the following Amazon S3 metadata:

- Key: Content-Encoding
- Value: gzip

If you upload the file using the AWS Management Console, the metadata is typically applied by the system. For information about uploading files to Amazon S3 using the AWS Management Console, the AWS CLI, or the API, see [Uploading objects in the Amazon Simple Storage Service User Guide](#).

For more information about Amazon S3 metadata and details about system-provided metadata, see [Editing object metadata in the Amazon S3 console](#) in the *Amazon Simple Storage Service User Guide*.

Import the gzip file into your RDS for PostgreSQL DB instance as shown following.

```
postgres=> CREATE TABLE test_gzip(id int, a text, b text, c text, d text);
postgres=> SELECT aws_s3.table_import_from_s3(
    'test_gzip', '', '(format csv)',
    'myS3Bucket', 'test-data.gz', 'us-east-2'
);
```

Importing an encoded Amazon S3 file

The following example shows how to import a file from Amazon S3 that has Windows-1252 encoding.

```
postgres=> SELECT aws_s3.table_import_from_s3(
    'test_table', '', 'encoding ''WIN1252'''',
    aws_commons.create_s3_uri('sampleBucket', 'SampleFile', 'us-east-2')
);
```

Function reference

Functions

- [aws_s3.table_import_from_s3 \(p. 1873\)](#)
- [aws_commons.create_s3_uri \(p. 1876\)](#)
- [aws_commons.create_aws_credentials \(p. 1876\)](#)

[aws_s3.table_import_from_s3](#)

Imports Amazon S3 data into an Amazon RDS table. The aws_s3 extension provides the aws_s3.table_import_from_s3 function. The return value is text.

Syntax

The required parameters are `table_name`, `column_list` and `options`. These identify the database table and specify how the data is copied into the table.

You can also use the following parameters:

- The `s3_info` parameter specifies the Amazon S3 file to import. When you use this parameter, access to Amazon S3 is provided by an IAM role for the PostgreSQL DB instance.

```
aws_s3.table_import_from_s3 (
    table_name text,
    column_list text,
    options text,
    s3_info aws_commons._s3_uri_1
)
```

- The `credentials` parameter specifies the credentials to access Amazon S3. When you use this parameter, you don't use an IAM role.

```
aws_s3.table_import_from_s3 (
    table_name text,
    column_list text,
    options text,
    s3_info aws_commons._s3_uri_1,
    credentials aws_commons._aws_credentials_1
)
```

Parameters

table_name

A required text string containing the name of the PostgreSQL database table to import the data into.

column_list

A required text string containing an optional list of the PostgreSQL database table columns in which to copy the data. If the string is empty, all columns of the table are used. For an example, see [Importing an Amazon S3 file that uses a custom delimiter \(p. 1872\)](#).

options

A required text string containing arguments for the PostgreSQL COPY command. These arguments specify how the data is to be copied into the PostgreSQL table. For more details, see the [PostgreSQL COPY documentation](#).

s3_info

An `aws_commons._s3_uri_1` composite type containing the following information about the S3 object:

- `bucket` – The name of the Amazon S3 bucket containing the file.
- `file_path` – The Amazon S3 file name including the path of the file.
- `region` – The AWS Region that the file is in. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

credentials

An `aws_commons._aws_credentials_1` composite type containing the following credentials to use for the import operation:

- Access key
- Secret key
- Session token

For information about creating an `aws_commons._aws_credentials_1` composite structure, see [aws_commons.create_aws_credentials \(p. 1876\)](#).

Alternate syntax

To help with testing, you can use an expanded set of parameters instead of the `s3_info` and `credentials` parameters. Following are additional syntax variations for the `aws_s3.table_import_from_s3` function:

- Instead of using the `s3_info` parameter to identify an Amazon S3 file, use the combination of the `bucket`, `file_path`, and `region` parameters. With this form of the function, access to Amazon S3 is provided by an IAM role on the PostgreSQL DB instance.

```
aws_s3.table_import_from_s3 (
    table_name text,
    column_list text,
    options text,
    bucket text,
    file_path text,
    region text
)
```

- Instead of using the `credentials` parameter to specify Amazon S3 access, use the combination of the `access_key`, `session_key`, and `session_token` parameters.

```
aws_s3.table_import_from_s3 (
    table_name text,
    column_list text,
    options text,
    bucket text,
    file_path text,
    region text,
    access_key text,
    secret_key text,
    session_token text
)
```

Alternate parameters

bucket

A text string containing the name of the Amazon S3 bucket that contains the file.

file_path

A text string containing the Amazon S3 file name including the path of the file.

region

A text string identifying the AWS Region location of the file. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

access_key

A text string containing the access key to use for the import operation. The default is NULL.

secret_key

A text string containing the secret key to use for the import operation. The default is NULL.

session_token

(Optional) A text string containing the session key to use for the import operation. The default is NULL.

aws_commons.create_s3_uri

Creates an `aws_commons._s3_uri_1` structure to hold Amazon S3 file information. Use the results of the `aws_commons.create_s3_uri` function in the `s3_info` parameter of the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function.

Syntax

```
aws_commons.create_s3_uri(  
    bucket text,  
    file_path text,  
    region text  
)
```

Parameters

bucket

A required text string containing the Amazon S3 bucket name for the file.

file_path

A required text string containing the Amazon S3 file name including the path of the file.

region

A required text string containing the AWS Region that the file is in. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

aws_commons.create_aws_credentials

Sets an access key and secret key in an `aws_commons._aws_credentials_1` structure. Use the results of the `aws_commons.create_aws_credentials` function in the `credentials` parameter of the [aws_s3.table_import_from_s3 \(p. 1873\)](#) function.

Syntax

```
aws_commons.create_aws_credentials(  
    access_key text,  
    secret_key text,  
    session_token text  
)
```

Parameters

access_key

A required text string containing the access key to use for importing an Amazon S3 file. The default is NULL.

secret_key

A required text string containing the secret key to use for importing an Amazon S3 file. The default is NULL.

session_token

An optional text string containing the session token to use for importing an Amazon S3 file. The default is NULL. If you provide an optional *session_token*, you can use temporary credentials.

Transporting PostgreSQL databases between DB instances

By using PostgreSQL transportable databases for Amazon RDS, you can move a PostgreSQL database between two DB instances. This is a very fast way to migrate large databases between different DB instances. To use this approach, your DB instances must both run the same major version of PostgreSQL.

This capability requires that you install the `pg_transport` extension on both the source and the destination DB instance. The `pg_transport` extension provides a physical transport mechanism that moves the database files with minimal processing. This mechanism moves data much faster than traditional dump and load processes, with less downtime.

Note

PostgreSQL transportable databases are available in RDS for PostgreSQL 11.5 and higher, and RDS for PostgreSQL version 10.10 and higher.

To transport a PostgreSQL DB instance from one RDS for PostgreSQL DB instance to another, you first set up the source and destination instances as detailed in [Setting up a DB instance for transport \(p. 1878\)](#). You can then transport the database by using the function described in [Transporting a PostgreSQL database \(p. 1879\)](#).

Topics

- [Limitations for using PostgreSQL transportable databases \(p. 1877\)](#)
- [Setting up to transport a PostgreSQL database \(p. 1878\)](#)
- [Transporting a PostgreSQL database to the destination from the source \(p. 1879\)](#)
- [What happens during database transport \(p. 1880\)](#)
- [Transportable databases function reference \(p. 1881\)](#)
- [Transportable databases parameter reference \(p. 1882\)](#)

Limitations for using PostgreSQL transportable databases

Transportable databases have the following limitations:

- **Read replicas** – You can't use transportable databases on read replicas or parent instances of read replicas.
- **Unsupported column types** – You can't use the `reg` data types in any database tables that you plan to transport with this method. These types depend on system catalog object IDs (OIDs), which often change during transport.
- **Tablespaces** – All source database objects must be in the default `pg_default` tablespace.
- **Compatibility** – Both the source and destination DB instances must run the same major version of PostgreSQL.
- **Extensions** – The source DB instance can have only the `pg_transport` installed.

- **Roles and ACLs** – The source database's access privileges and ownership information aren't carried over to the destination database. All database objects are created and owned by the local destination user of the transport.
- **Concurrent transports** – A single DB instance can support up to 32 concurrent transports, including both imports and exports, if worker processes have been configured properly.
- **RDS for PostgreSQL DB instances only** – PostgreSQL transportable databases are supported on RDS for PostgreSQL DB instances only. You can't use it with on-premises databases or databases running on Amazon EC2.

Setting up to transport a PostgreSQL database

Before you begin, make sure that your RDS for PostgreSQL DB instances meet the following requirements:

- The RDS for PostgreSQL DB instances for source and destination must run the same version of PostgreSQL.
- The destination DB can't have a database of the same name as the source DB that you want to transport.
- The account you use to run the transport needs `rds_superuser` privileges on both the source DB and the destination DB.
- The security group for the source DB instance must allow inbound access from the destination DB instance. This might already be the case if your source and destination DB instances are located in the VPC. For more information about security groups, see [Controlling access with security groups \(p. 2085\)](#).

Transporting databases from a source DB instance to a destination DB instance requires several changes to the DB parameter group associated with each instance. That means that you must create a custom DB parameter group for the source DB instance and create a custom DB parameter group for the destination DB instance.

Note

If your DB instances are already configured using custom DB parameter groups, you can start with step 2 in the following procedure.

To configure the custom DB group parameters for transporting databases

For the following steps, use an account that has `rds_superuser` privileges.

1. If the source and destination DB instances use a default DB parameter group, you need to create a custom DB parameter using the appropriate version for your instances. You do this so you can change values for several parameters. For more information, see [Working with parameter groups \(p. 289\)](#).
2. In the custom DB parameter group, change values for the following parameters:
 - `shared_preload_libraries` – Add `pg_transport` to the list of libraries.
 - `pg_transport.num_workers` – The default value is 3. Increase or reduce this value as needed for your database. For a 200 GB database, we recommend no larger than 8. Keep in mind that if you increase the default value for this parameter, you should also increase the value of `max_worker_processes`.
 - `pg_transport.work_mem` – The default value is either 128 MB or 256 MB, depending on the PostgreSQL version. The default setting can typically be left unchanged.
 - `max_worker_processes` – The value of this parameter needs to be set using the following calculation:

```
3 * pg_transport.num_workers) + 9
```

This value is required on the destination to handle various background worker processes involved in the transport. To learn more about `max_worker_processes`, see [Resource Consumption](#) in the PostgreSQL documentation.

For more information about `pg_transport` parameters, see [Transportable databases parameter reference \(p. 1882\)](#).

3. Reboot the source RDS for PostgreSQL DB instance and the destination instance so that the settings for the parameters take effect.
4. Connect to your RDS for PostgreSQL source DB instance.

```
psql --host=source-instance.111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres --password
```

5. Remove extraneous extensions from the public schema of the DB instance. Only the `pg_transport` extension is allowed during the actual transport operation.
6. Install the `pg_transport` extension as follows:

```
postgres=> CREATE EXTENSION pg_transport;
CREATE EXTENSION
```

7. Connect to your RDS for PostgreSQL destination DB instance. Remove any extraneous extensions, and then install the `pg_transport` extension.

```
postgres=> CREATE EXTENSION pg_transport;
CREATE EXTENSION
```

Transporting a PostgreSQL database to the destination from the source

After you complete the process described in [Setting up to transport a PostgreSQL database \(p. 1878\)](#), you can start the transport. To do so, run the `transport.import_from_server` function on the destination DB instance. In the syntax following you can find the function parameters.

```
SELECT transport.import_from_server(
    'source-db-instance-endpoint',
    'source-db-instance-port',
    'source-db-instance-user',
    'source-user-password',
    'source-database-name',
    'destination-user-password',
    false);
```

The `false` value shown in the example tells the function that this is not a dry run. To test your transport setup, you can specify `true` for the `dry_run` option when you call the function, as shown following:

```
postgres=> SELECT transport.import_from_server(
    'docs-lab-source-db.666666666666aws-region.rds.amazonaws.com', 5432,
    'postgres', '*****', 'labdb', '*****', true);
INFO: Starting dry-run of import of database "labdb".
INFO: Created connections to remote database (took 0.03 seconds).
INFO: Checked remote cluster compatibility (took 0.05 seconds).
```

```
INFO: Dry-run complete                                (took 0.08 seconds total).
      import_from_server
-----
(1 row)
```

The INFO lines are output because the `pg_transport.timing` parameter is set to its default value, `true`. Set the `dry_run` to `false` when you run the command and the source database is imported to the destination, as shown following:

```
INFO: Starting import of database "labdb".
INFO: Created connections to remote database      (took 0.02 seconds).
INFO: Marked remote database as read only        (took 0.13 seconds).
INFO: Checked remote cluster compatibility        (took 0.03 seconds).
INFO: Signaled creation of PITR blackout window (took 2.01 seconds).
INFO: Applied remote database schema pre-data    (took 0.50 seconds).
INFO: Created connections to local cluster       (took 0.01 seconds).
INFO: Locked down destination database           (took 0.00 seconds).
INFO: Completed transfer of database files       (took 0.24 seconds).
INFO: Completed clean up                         (took 1.02 seconds).
INFO: Physical transport complete                (took 3.97 seconds total).
      import_from_server
-----
(1 row)
```

This function requires that you provide database user passwords. Thus, we recommend that you change the passwords of the user roles you used after transport is complete. Or, you can use SQL bind variables to create temporary user roles. Use these temporary roles for the transport and then discard the roles afterwards.

If your transport isn't successful, you might see an error message similar to the following:

```
pg_transport.num_workers=8 25% of files transported failed to download file data
```

The "failed to download file data" error message indicates that the number of worker processes isn't set correctly for the size of the database. You might need to increase or decrease the value set for `pg_transport.num_workers`. Each failure reports the percentage of completion, so you can see the impact of your changes. For example, changing the setting from 8 to 4 in one case resulted in the following:

```
pg_transport.num_workers=4 75% of files transported failed to download file data
```

Keep in mind that the `max_worker_processes` parameter is also taken into account during the transport process. In other words, you might need to modify both `pg_transport.num_workers` and `max_worker_processes` to successfully transport the database. The example shown finally worked when the `pg_transport.num_workers` was set to 2:

```
pg_transport.num_workers=2 100% of files transported
```

For more information about the `transport.import_from_server` function and its parameters, see [Transportable databases function reference \(p. 1881\)](#).

What happens during database transport

The PostgreSQL transportable databases feature uses a pull model to import the database from the source DB instance to the destination. The `transport.import_from_server` function creates the in-

transit database on the destination DB instance. The in-transit database is inaccessible on the destination DB instance for the duration of the transport.

When transport begins, all current sessions on the source database are ended. Any databases other than the source database on the source DB instance aren't affected by the transport.

The source database is put into a special read-only mode. While it's in this mode, you can connect to the source database and run read-only queries. However, write-enabled queries and some other types of commands are blocked. Only the specific source database that is being transported is affected by these restrictions.

During transport, you can't restore the destination DB instance to a point in time. This is because the transport isn't transactional and doesn't use the PostgreSQL write-ahead log to record changes. If the destination DB instance has automatic backups enabled, a backup is automatically taken after transport completes. Point-in-time restores are available for times *after* the backup finishes.

If the transport fails, the `pg_transport` extension attempts to undo all changes to the source and destination DB instances. This includes removing the destination's partially transported database. Depending on the type of failure, the source database might continue to reject write-enabled queries. If this happens, use the following command to allow write-enabled queries.

```
ALTER DATABASE db-name SET default_transaction_read_only = false;
```

Transportable databases function reference

The `transport.import_from_server` function transports a PostgreSQL database by importing it from a source DB instance to a destination DB instance. It does this by using a physical database connection transport mechanism.

Before starting the transport, this function verifies that the source and the destination DB instances are the same version and are compatible for the migration. It also confirms that the destination DB instance has enough space for the source.

Syntax

```
transport.import_from_server(
    host text,
    port int,
    username text,
    password text,
    database text,
    local_password text,
    dry_run bool
)
```

Return Value

None.

Parameters

You can find descriptions of the `transport.import_from_server` function parameters in the following table.

Parameter	Description
host	The endpoint of the source DB instance.

Parameter	Description
port	An integer representing the port of the source DB instance. PostgreSQL DB instances often use port 5432.
username	The user of the source DB instance. This user must be a member of the <code>rds_superuser</code> role.
password	The user password of the source DB instance.
database	The name of the database in the source DB instance to transport.
local_password	The local password of the current user for the destination DB instance. This user must be a member of the <code>rds_superuser</code> role.
dry_run	An optional Boolean value specifying whether to perform a dry run. The default is <code>false</code> , which means the transport proceeds. To confirm compatibility between the source and destination DB instances without performing the actual transport, set <code>dry_run</code> to <code>true</code> .

Example

For an example, see [Transporting a PostgreSQL database to the destination from the source \(p. 1879\)](#).

Transportable databases parameter reference

Several parameters control the behavior of the `pg_transport` extension. Following, you can find descriptions of these parameters.

`pg_transport.num_workers`

The number of workers to use for the transport process. The default is 3. Valid values are 1–32. Even the largest database transports typically require fewer than 8 workers. The value of this setting on the destination DB instance is used by both destination and source during transport.

`pg_transport.timing`

Specifies whether to report timing information during the transport. The default is `true`, meaning that timing information is reported. We recommend that you leave this parameter set to `true` so you can monitor progress. For example output, see [Transporting a PostgreSQL database to the destination from the source \(p. 1879\)](#).

`pg_transport.work_mem`

The maximum amount of memory to allocate for each worker. The default is 131072 kilobytes (KB) or 262144 KB (256 MB), depending on the PostgreSQL version. The minimum value is 64 megabytes (65536 KB). Valid values are in kilobytes (KBs) as binary base-2 units, where 1 KB = 1024 bytes.

The transport might use less memory than is specified in this parameter. Even large database transports typically require less than 256 MB (262144 KB) of memory per worker.

Exporting data from an RDS for PostgreSQL DB instance to Amazon S3

You can query data from an RDS for PostgreSQL DB instance and export it directly into files stored in an Amazon S3 bucket. To do this, you first install the RDS for PostgreSQL `aws_s3` extension. This extension provides you with the functions that you use to export the results of queries to Amazon S3. Following, you can find out how to install the extension and how to export data to Amazon S3.

You can export from a provisioned or an Aurora Serverless v2 DB instance. These steps aren't supported for Aurora Serverless v1.

Note

Cross-account export to Amazon S3 isn't supported.

All currently available versions of RDS for PostgreSQL support exporting data to Amazon Simple Storage Service. For detailed version information, see [Amazon RDS for PostgreSQL updates](#) in the *Amazon RDS for PostgreSQL Release Notes*.

If you don't have a bucket set up for your export, see the following topics the *Amazon Simple Storage Service User Guide*.

- [Setting up Amazon S3](#)
- [Create a bucket](#)

The upload to Amazon S3 uses server-side encryption by default. If you are using encryption, the Amazon S3 bucket must be encrypted with an AWS managed key. Currently, you can't export data to a bucket that's encrypted with a customer managed key.

Note

You can save DB snapshot data to Amazon S3 using the AWS Management Console, AWS CLI, or Amazon RDS API. For more information, see [Exporting DB snapshot data to Amazon S3 \(p. 481\)](#).

Topics

- [Installing the aws_s3 extension \(p. 1883\)](#)
- [Overview of exporting data to Amazon S3 \(p. 1884\)](#)
- [Specifying the Amazon S3 file path to export to \(p. 1885\)](#)
- [Setting up access to an Amazon S3 bucket \(p. 1886\)](#)
- [Exporting query data using the aws_s3.query_export_to_s3 function \(p. 1889\)](#)
- [Troubleshooting access to Amazon S3 \(p. 1891\)](#)
- [Function reference \(p. 1891\)](#)

Installing the aws_s3 extension

Before you can use Amazon Simple Storage Service with your RDS for PostgreSQL DB instance, you need to install the `aws_s3` extension. This extension provides functions for exporting data from an RDS for PostgreSQL DB instance to an Amazon S3 bucket. It also provides functions for importing data from an Amazon S3. For more information, see [Importing data from Amazon S3 into an RDS for PostgreSQL DB instance \(p. 1864\)](#). The `aws_s3` extension depends on some of the helper functions in the `aws_commons` extension, which is installed automatically when needed.

To install the aws_s3 extension

1. Use psql (or pgAdmin) to connect to the RDS for PostgreSQL DB instance as a user that has rds_superuser privileges. If you kept the default name during the setup process, you connect as postgres.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres  
--password
```

2. To install the extension, run the following command.

```
postgres=> CREATE EXTENSION aws_s3 CASCADE;  
NOTICE: installing required extension "aws_commons"  
CREATE EXTENSION
```

3. To verify that the extension is installed, you can use the psql \dx metacommand.

```
postgres=> \dx  
      List of installed extensions  
 Name | Version | Schema | Description  
-----+-----+-----+  
aws_commons | 1.2 | public | Common data types across AWS services  
aws_s3 | 1.1 | public | AWS S3 extension for importing data from S3  
plpgsql | 1.0 | pg_catalog | PL/pgSQL procedural language  
(3 rows)
```

The functions for importing data from Amazon S3 and exporting data to Amazon S3 are now available to use.

Verify that your RDS for PostgreSQL version supports exports to Amazon S3

You can verify that your RDS for PostgreSQL version supports export to Amazon S3 by using the describe-db-engine-versions command. The following example verifies support for version 10.14.

```
aws rds describe-db-engine-versions --region us-east-1 ^  
--engine postgres --engine-version 10.14 | grep s3Export
```

If the output includes the string "s3Export", then the engine supports Amazon S3 exports. Otherwise, the engine doesn't support them.

Overview of exporting data to Amazon S3

To export data stored in an RDS for PostgreSQL database to an Amazon S3 bucket, use the following procedure.

To export RDS for PostgreSQL data to S3

1. Identify an Amazon S3 file path to use for exporting data. For details about this process, see [Specifying the Amazon S3 file path to export to \(p. 1885\)](#).
2. Provide permission to access the Amazon S3 bucket.

To export data to an Amazon S3 file, give the RDS for PostgreSQL DB instance permission to access the Amazon S3 bucket that the export will use for storage. Doing this includes the following steps:

1. Create an IAM policy that provides access to an Amazon S3 bucket that you want to export to.

2. Create an IAM role.
3. Attach the policy you created to the role you created.
4. Add this IAM role to your DB instance.

For details about this process, see [Setting up access to an Amazon S3 bucket \(p. 1886\)](#).

3. Identify a database query to get the data. Export the query data by calling the `aws_s3.query_export_to_s3` function.

After you complete the preceding preparation tasks, use the `aws_s3.query_export_to_s3` (p. 1891) function to export query results to Amazon S3. For details about this process, see [Exporting query data using the aws_s3.query_export_to_s3 function \(p. 1889\)](#).

Specifying the Amazon S3 file path to export to

Specify the following information to identify the location in Amazon S3 where you want to export data to:

- Bucket name – A *bucket* is a container for Amazon S3 objects or files.

For more information on storing data with Amazon S3, see [Create a bucket](#) and [View an object](#) in the *Amazon Simple Storage Service User Guide*.

- File path – The file path identifies where the export is stored in the Amazon S3 bucket. The file path consists of the following:
 - An optional path prefix that identifies a virtual folder path.
 - A file prefix that identifies one or more files to be stored. Larger exports are stored in multiple files, each with a maximum size of approximately 6 GB. The additional file names have the same file prefix but with `_partXX` appended. The `XX` represents 2, then 3, and so on.

For example, a file path with an exports folder and a query-1-export file prefix is `/exports/query-1-export`.

- AWS Region (optional) – The AWS Region where the Amazon S3 bucket is located. If you don't specify an AWS Region value, then Amazon RDS saves your files into Amazon S3 in the same AWS Region as the exporting DB instance.

Note

Currently, the AWS Region must be the same as the region of the exporting DB instance.

For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

To hold the Amazon S3 file information about where the export is to be stored, you can use the `aws_commons.create_s3_uri` (p. 1893) function to create an `aws_commons._s3_uri_1` composite structure as follows.

```
psql=> SELECT aws_commons.create_s3_uri(  
    'sample-bucket',  
    'sample-filepath',  
    'us-west-2'  
) AS s3_uri_1 \gset
```

You later provide this `s3_uri_1` value as a parameter in the call to the `aws_s3.query_export_to_s3` (p. 1891) function. For examples, see [Exporting query data using the aws_s3.query_export_to_s3 function \(p. 1889\)](#).

Setting up access to an Amazon S3 bucket

To export data to Amazon S3, give your PostgreSQL DB instance permission to access the Amazon S3 bucket that the files are to go in.

To do this, use the following procedure.

To give a PostgreSQL DB instance access to Amazon S3 through an IAM role

1. Create an IAM policy.

This policy provides the bucket and object permissions that allow your PostgreSQL DB instance to access Amazon S3.

As part of creating this policy, take the following steps:

- a. Include in the policy the following required actions to allow the transfer of files from your PostgreSQL DB instance to an Amazon S3 bucket:
 - `s3:PutObject`
 - `s3:AbortMultipartUpload`
- b. Include the Amazon Resource Name (ARN) that identifies the Amazon S3 bucket and objects in the bucket. The ARN format for accessing Amazon S3 is: `arn:aws:s3:::your-s3-bucket/*`

For more information on creating an IAM policy for Amazon RDS for PostgreSQL, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#). See also [Tutorial: Create and attach your first customer managed policy](#) in the *IAM User Guide*.

The following AWS CLI command creates an IAM policy named `rds-s3-export-policy` with these options. It grants access to a bucket named `your-s3-bucket`.

Warning

We recommend that you set up your database within a private VPC that has endpoint policies configured for accessing specific buckets. For more information, see [Using endpoint policies for Amazon S3](#) in the Amazon VPC User Guide.

We strongly recommend that you do not create a policy with all-resource access. This access can pose a threat for data security. If you create a policy that gives `S3:PutObject` access to all resources using "Resource": "*", then a user with export privileges can export data to all buckets in your account. In addition, the user can export data to *any publicly writable bucket within your AWS Region*.

After you create the policy, note the Amazon Resource Name (ARN) of the policy. You need the ARN for a subsequent step when you attach the policy to an IAM role.

```
aws iam create-policy --policy-name rds-s3-export-policy --policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "s3export",  
            "Action": [  
                "s3:PutObject",  
                "s3:AbortMultipartUpload"  
            ],  
            "Effect": "Allow",  
            "Resource": [  
                "arn:aws:s3:::your-s3-bucket/*"  
            ]  
        }  
    ]  
}
```

```
}
```

2. Create an IAM role.

You do this so Amazon RDS can assume this IAM role on your behalf to access your Amazon S3 buckets. For more information, see [Creating a role to delegate permissions to an IAM user](#) in the *IAM User Guide*.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource-based policies to limit the service's permissions to a specific resource. This is the most effective way to protect against the [confused deputy problem](#).

If you use both global condition context keys and the `aws:SourceArn` value contains the account ID, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

- Use `aws:SourceArn` if you want cross-service access for a single resource.
- Use `aws:SourceAccount` if you want to allow any resource in that account to be associated with the cross-service use.

In the policy, be sure to use the `aws:SourceArn` global condition context key with the full ARN of the resource. The following example shows how to do so using the AWS CLI command to create a role named `rds-s3-export-role`.

Example

For Linux, macOS, or Unix:

```
aws iam create-role \
--role-name rds-s3-export-role \
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
            }
        }
    ]
}'
```

For Windows:

```
aws iam create-role ^
--role-name rds-s3-export-role ^
--assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
            }
        }
    ]
}'
```

```
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
            }
        }
    ]'
}'
```

3. Attach the IAM policy that you created to the IAM role that you created.

The following AWS CLI command attaches the policy created earlier to the role named `rds-s3-export-role`. Replace `your-policy-arn` with the policy ARN that you noted in an earlier step.

```
aws iam attach-role-policy --policy-arn your-policy-arn --role-name rds-s3-export-role
```

4. Add the IAM role to the DB instance. You do so by using the AWS Management Console or AWS CLI, as described following.

Console

To add an IAM role for a PostgreSQL DB instance using the console

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. Choose the PostgreSQL DB instance name to display its details.
3. On the **Connectivity & security** tab, in the **Manage IAM roles** section, choose the role to add under **Add IAM roles to this instance**.
4. Under **Feature**, choose **s3Export**.
5. Choose **Add role**.

AWS CLI

To add an IAM role for a PostgreSQL DB instance using the CLI

- Use the following command to add the role to the PostgreSQL DB instance named `my-db-instance`. Replace `your-role-arn` with the role ARN that you noted in a previous step. Use `s3Export` for the value of the `--feature-name` option.

Example

For Linux, macOS, or Unix:

```
aws rds add-role-to-db-instance \
--db-instance-identifier my-db-instance \
--feature-name s3Export \
--role-arn your-role-arn \
--region your-region
```

For Windows:

```
aws rds add-role-to-db-instance ^
```

```
--db-instance-identifier my-db-instance ^
--feature-name s3Export ^
--role-arn your-role-arn ^
--region your-region
```

Exporting query data using the `aws_s3.query_export_to_s3` function

Export your PostgreSQL data to Amazon S3 by calling the [aws_s3.query_export_to_s3 \(p. 1891\)](#) function.

Topics

- [Prerequisites \(p. 1889\)](#)
- [Calling aws_s3.query_export_to_s3 \(p. 1889\)](#)
- [Exporting to a CSV file that uses a custom delimiter \(p. 1890\)](#)
- [Exporting to a binary file with encoding \(p. 1891\)](#)

Prerequisites

Before you use the `aws_s3.query_export_to_s3` function, be sure to complete the following prerequisites:

- Install the required PostgreSQL extensions as described in [Overview of exporting data to Amazon S3 \(p. 1884\)](#).
- Determine where to export your data to Amazon S3 as described in [Specifying the Amazon S3 file path to export to \(p. 1885\)](#).
- Make sure that the DB instance has export access to Amazon S3 as described in [Setting up access to an Amazon S3 bucket \(p. 1886\)](#).

The examples following use a database table called `sample_table`. These examples export the data into a bucket called `sample-bucket`. The example table and data are created with the following SQL statements in `psql`.

```
psql=> CREATE TABLE sample_table (bid bigint PRIMARY KEY, name varchar(80));
psql=> INSERT INTO sample_table (bid,name) VALUES (1, 'Monday'), (2,'Tuesday'), (3,
'Wednesday');
```

Calling aws_s3.query_export_to_s3

The following shows the basic ways of calling the [aws_s3.query_export_to_s3 \(p. 1891\)](#) function.

These examples use the variable `s3_uri_1` to identify a structure that contains the information identifying the Amazon S3 file. Use the [aws_commons.create_s3_uri \(p. 1893\)](#) function to create the structure.

```
psql=> SELECT aws_commons.create_s3_uri(
  'sample-bucket',
  'sample-filepath',
  'us-west-2'
) AS s3_uri_1 \gset
```

Although the parameters vary for the following two aws_s3.query_export_to_s3 function calls, the results are the same for these examples. All rows of the sample_table table are exported into a bucket called sample-bucket.

```
psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM sample_table', :'s3_uri_1');

psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM sample_table', :'s3_uri_1',
options :='format text');
```

The parameters are described as follows:

- 'SELECT * FROM sample_table' – The first parameter is a required text string containing an SQL query. The PostgreSQL engine runs this query. The results of the query are copied to the S3 bucket identified in other parameters.
- ':s3_uri_1' – This parameter is a structure that identifies the Amazon S3 file. This example uses a variable to identify the previously created structure. You can instead create the structure by including the aws_commons.create_s3_uri function call inline within the aws_s3.query_export_to_s3 function call as follows.

```
SELECT * from aws_s3.query_export_to_s3('select * from sample_table',
aws_commons.create_s3_uri('sample-bucket', 'samplefilepath', 'us-west-2')
);
```

- options :='format text' – The options parameter is an optional text string containing PostgreSQL COPY arguments. The copy process uses the arguments and format of the [PostgreSQL COPY](#) command.

If the file specified doesn't exist in the Amazon S3 bucket, it's created. If the file already exists, it's overwritten. The syntax for accessing the exported data in Amazon S3 is the following.

```
s3-region://bucket-name[/path-prefix]/file-prefix
```

Larger exports are stored in multiple files, each with a maximum size of approximately 6 GB. The additional file names have the same file prefix but with _partXX appended. The XX represents 2, then 3, and so on. For example, suppose that you specify the path where you store data files as the following.

```
s3-us-west-2://my-bucket/my-prefix
```

If the export has to create three data files, the Amazon S3 bucket contains the following data files.

```
s3-us-west-2://my-bucket/my-prefix
s3-us-west-2://my-bucket/my-prefix_part2
s3-us-west-2://my-bucket/my-prefix_part3
```

For the full reference for this function and additional ways to call it, see [aws_s3.query_export_to_s3 \(p. 1891\)](#). For more about accessing files in Amazon S3, see [View an object](#) in the [Amazon Simple Storage Service User Guide](#).

Exporting to a CSV file that uses a custom delimiter

The following example shows how to call the [aws_s3.query_export_to_s3 \(p. 1891\)](#) function to export data to a file that uses a custom delimiter. The example uses arguments of the [PostgreSQL COPY](#) command to specify the comma-separated value (CSV) format and a colon (:) delimiter.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
options :='format csv, delimiter $$:$>');
```

Exporting to a binary file with encoding

The following example shows how to call the [aws_s3.query_export_to_s3 \(p. 1891\)](#) function to export data to a binary file that has Windows-1253 encoding.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
options :='format binary, encoding WIN1253');
```

Troubleshooting access to Amazon S3

If you encounter connection problems when attempting to export data to Amazon S3, first confirm that the outbound access rules for the VPC security group associated with your DB instance permit network connectivity. Specifically, the security group must have a rule that allows the DB instance to send TCP traffic to port 443 and to any IPv4 addresses (0.0.0.0/0). For more information, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

See also the following for recommendations:

- [Troubleshooting Amazon RDS identity and access \(p. 2075\)](#)
- [Troubleshooting Amazon S3 in the Amazon Simple Storage Service User Guide](#)
- [Troubleshooting Amazon S3 and IAM in the IAM User Guide](#)

Function reference

Functions

- [aws_s3.query_export_to_s3 \(p. 1891\)](#)
- [aws_commons.create_s3_uri \(p. 1893\)](#)

aws_s3.query_export_to_s3

Exports a PostgreSQL query result to an Amazon S3 bucket. The aws_s3 extension provides the aws_s3.query_export_to_s3 function.

The two required parameters are query and s3_info. These define the query to be exported and identify the Amazon S3 bucket to export to. An optional parameter called options provides for defining various export parameters. For examples of using the aws_s3.query_export_to_s3 function, see [Exporting query data using the aws_s3.query_export_to_s3 function \(p. 1889\)](#).

Syntax

```
aws_s3.query_export_to_s3(
    query text,
    s3_info aws_commons._s3_uri_1,
    options text
)
```

Input parameters

query

A required text string containing an SQL query that the PostgreSQL engine runs. The results of this query are copied to an S3 bucket identified in the *s3_info* parameter.

s3_info

An `aws_commons._s3_uri_1` composite type containing the following information about the S3 object:

- `bucket` – The name of the Amazon S3 bucket to contain the file.
- `file_path` – The Amazon S3 file name and path.
- `region` – The AWS Region that the bucket is in. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

Currently, this value must be the same AWS Region as that of the exporting DB instance. The default is the AWS Region of the exporting DB instance.

To create an `aws_commons._s3_uri_1` composite structure, see the [aws_commons.create_s3_uri \(p. 1893\)](#) function.

options

An optional text string containing arguments for the PostgreSQL COPY command. These arguments specify how the data is to be copied when exported. For more details, see the [PostgreSQL COPY documentation](#).

Alternate input parameters

To help with testing, you can use an expanded set of parameters instead of the *s3_info* parameter. Following are additional syntax variations for the `aws_s3.query_export_to_s3` function.

Instead of using the *s3_info* parameter to identify an Amazon S3 file, use the combination of the `bucket`, `file_path`, and `region` parameters.

```
aws_s3.query_export_to_s3(  
    query text,  
    bucket text,  
    file_path text,  
    region text,  
    options text  
)
```

query

A required text string containing an SQL query that the PostgreSQL engine runs. The results of this query are copied to an S3 bucket identified in the *s3_info* parameter.

bucket

A required text string containing the name of the Amazon S3 bucket that contains the file.

file_path

A required text string containing the Amazon S3 file name including the path of the file.

region

An optional text string containing the AWS Region that the bucket is in. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

Currently, this value must be the same AWS Region as that of the exporting DB instance. The default is the AWS Region of the exporting DB instance.

options

An optional text string containing arguments for the PostgreSQL COPY command. These arguments specify how the data is to be copied when exported. For more details, see the [PostgreSQL COPY documentation](#).

Output parameters

```
aws_s3.query_export_to_s3(  
    OUT rows_uploaded bigint,  
    OUT files_uploaded bigint,  
    OUT bytes_uploaded bigint  
)
```

rows_uploaded

The number of table rows that were successfully uploaded to Amazon S3 for the given query.

files_uploaded

The number of files uploaded to Amazon S3. Files are created in sizes of approximately 6 GB. Each additional file created has `_partXX` appended to the name. The `XX` represents 2, then 3, and so on as needed.

bytes_uploaded

The total number of bytes uploaded to Amazon S3.

Examples

```
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-  
bucket', 'samplefilepath');  
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-  
bucket', 'samplefilepath','us-west-2');  
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'sample-  
bucket', 'samplefilepath','us-west-2','format text');
```

aws_commons.create_s3_uri

Creates an `aws_commons._s3_uri_1` structure to hold Amazon S3 file information. You use the results of the `aws_commons.create_s3_uri` function in the `s3_info` parameter of the [aws_s3.query_export_to_s3 \(p. 1891\)](#) function. For an example of using the `aws_commons.create_s3_uri` function, see [Specifying the Amazon S3 file path to export to \(p. 1885\)](#).

Syntax

```
aws_commons.create_s3_uri(  
    bucket text,  
    file_path text,  
    region text  
)
```

Input parameters

bucket

A required text string containing the Amazon S3 bucket name for the file.

file_path

A required text string containing the Amazon S3 file name including the path of the file.

region

A required text string containing the AWS Region that the file is in. For a listing of AWS Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

Invoking an AWS Lambda function from an RDS for PostgreSQL DB instance

AWS Lambda is an event-driven compute service that lets you run code without provisioning or managing servers. It's available for use with many AWS services, including RDS for PostgreSQL. For example, you can use Lambda functions to process event notifications from a database, or to load data from files whenever a new file is uploaded to Amazon S3. To learn more about Lambda, see [What is AWS Lambda?](#) in the *AWS Lambda Developer Guide*.

Note

Invoking an AWS Lambda function is supported in these RDS for PostgreSQL versions:

- 14.1 and higher minor versions
- 13.2 and higher minor versions
- 12.6 and higher minor versions

Setting up RDS for PostgreSQL to work with Lambda functions is a multi-step process involving AWS Lambda, IAM, your VPC, and your RDS for PostgreSQL DB instance. Following, you can find summaries of the necessary steps.

For more information about Lambda functions, see [Getting started with Lambda](#) and [AWS Lambda foundations](#) in the *AWS Lambda Developer Guide*.

Topics

- [Step 1: Configure your RDS for PostgreSQL DB instance for outbound connections to AWS Lambda \(p. 1895\)](#)
- [Step 2: Configure IAM for your RDS for PostgreSQL DB instance and AWS Lambda \(p. 1896\)](#)
- [Step 3: Install the aws_lambda extension for an RDS for PostgreSQL DB instance \(p. 1897\)](#)
- [Step 4: Use Lambda helper functions with your RDS for PostgreSQL DB instance \(Optional\) \(p. 1898\)](#)
- [Step 5: Invoke a Lambda function from your RDS for PostgreSQL DB instance \(p. 1898\)](#)
- [Step 6: Grant other users permission to invoke Lambda functions \(p. 1899\)](#)
- [Examples: Invoking Lambda functions from your RDS for PostgreSQL DB instance \(p. 1900\)](#)
- [Lambda function error messages \(p. 1902\)](#)
- [AWS Lambda function reference \(p. 1903\)](#)

Step 1: Configure your RDS for PostgreSQL DB instance for outbound connections to AWS Lambda

Lambda functions always run inside an Amazon VPC that's owned by the AWS Lambda service. Lambda applies network access and security rules to this VPC and it maintains and monitors the VPC automatically. Your RDS for PostgreSQL DB instance sends network traffic to the Lambda service's VPC. How you configure this depends on whether your DB instance is public or private.

- **Public RDS for PostgreSQL DB instance** – A DB instance is public if it's located in a public subnet on your VPC, and if the instance's "PubliclyAccessible" property is true. To find the value of this property, you can use the [describe-db-instances](#) AWS CLI command. Or, you can use the AWS Management Console to open the **Connectivity & security** tab and check that **Publicly accessible** is Yes. To verify that the instance is in the public subnet of your VPC, you can use the AWS Management Console or the AWS CLI.

To set up access to Lambda, you use the AWS Management Console or the AWS CLI to create an outbound rule on your VPC's security group. The outbound rule specifies that TCP can use port 443 to send packets to any IPv4 addresses (0.0.0.0/0).

- **Private RDS for PostgreSQL DB instance** – In this case, the instance's "PubliclyAccessible" property is false or it's in a private subnet. To allow the instance to work with Lambda, you can use a Network Address Translation (NAT) gateway. For more information, see [NAT gateways](#). Or, you can configure your VPC with a VPC endpoint for Lambda. For more information, see [VPC endpoints](#) in the *Amazon VPC User Guide*. The endpoint responds to calls made by your RDS for PostgreSQL DB instance to your Lambda functions. The VPC endpoint uses its own private DNS resolution. RDS for PostgreSQL can't use the Lambda VPC endpoint until you change the value of the `rds.custom_dns_resolution` from its default value of 0 (not enabled) to 1. To do so:
 - Create a custom DB parameter group.
 - Change the value of the `rds.custom_dns_resolution` parameter from its default of 0 to 1.
 - Modify your DB instance to use your custom DB parameter group.
 - Reboot the instance to have the modified parameter take effect.

Your VPC can now interact with the AWS Lambda VPC at the network level. Next, you configure the permissions using IAM.

Step 2: Configure IAM for your RDS for PostgreSQL DB instance and AWS Lambda

Invoking Lambda functions from your RDS for PostgreSQL DB instance requires certain privileges. To configure the necessary privileges, we recommend that you create an IAM policy that allows invoking Lambda functions, assign that policy to a role, and then apply the role to your DB instance. This approach gives the DB instance privileges to invoke the specified Lambda function on your behalf. The following steps show you how to do this using the AWS CLI.

To configure IAM permissions for using your Amazon RDS instance with Lambda

1. Use the [create-policy](#) AWS CLI command to create an IAM policy that allows your RDS for PostgreSQL DB instance to invoke the specified Lambda function. (The statement ID (Sid) is an optional description for your policy statement and has no effect on usage.) This policy gives your DB instance the minimum permissions needed to invoke the specified Lambda function.

```
aws iam create-policy --policy-name rds-lambda-policy --policy-document '{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowAccessToExampleFunction",  
            "Effect": "Allow",  
            "Action": "lambda:InvokeFunction",  
            "Resource": "arn:aws:lambda:aws-region:444455556666:function:my-function"  
        }  
    ]  
}'
```

Alternatively, you can use the predefined AWSLambdaRole policy that allows you to invoke any of your Lambda functions. For more information, see [Identity-based IAM policies for Lambda](#)

2. Use the [create-role](#) AWS CLI command to create an IAM role that the policy can assume at runtime.

```
aws iam create-role --role-name rds-lambda-role --assume-role-policy-document '{  
    "Version": "2012-10-17",  
}
```

```
"Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "Service": "rds.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }
]'
```

3. Apply the policy to the role by using the [attach-role-policy](#) AWS CLI command.

```
aws iam attach-role-policy \
--policy-arn arn:aws:iam::444455556666:policy/rds-lambda-policy \
--role-name rds-lambda-role --region aws-region
```

4. Apply the role to your RDS for PostgreSQL DB instance by using the [add-role-to-db-instance](#) AWS CLI command. This last step allows your DB instance's database users to invoke Lambda functions.

```
aws rds add-role-to-db-instance \
--db-cluster-identifier my-cluster-name \
--feature-name Lambda \
--role-arn arn:aws:iam::444455556666:role/rds-lambda-role \
--region aws-region
```

With the VPC and the IAM configurations complete, you can now install the `aws_lambda` extension. (Note that you can install the extension at any time, but until you set up the correct VPC support and IAM privileges, the `aws_lambda` extension adds nothing to your RDS for PostgreSQL DB instance's capabilities.)

Step 3: Install the `aws_lambda` extension for an RDS for PostgreSQL DB instance

To use AWS Lambda with your RDS for PostgreSQL DB instance, the `aws_lambda` PostgreSQL extension to your RDS for PostgreSQL. This extension provides your RDS for PostgreSQL DB instance with the ability to call Lambda functions from PostgreSQL.

To install the `aws_lambda` extension in your RDS for PostgreSQL DB instance

Use the PostgreSQL `psql` command-line or the pgAdmin tool to connect to your RDS for PostgreSQL DB instance.

1. Connect to your RDS for PostgreSQL DB instance as a user with `rds_superuser` privileges. The default `postgres` user is shown in the example.

```
psql -h instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
```

2. Install the `aws_lambda` extension. The `aws_commons` extension is also required. It provides helper functions to `aws_lambda` and many other Aurora extensions for PostgreSQL. If it's not already on your RDS for PostgreSQLDB instance, it's installed with `aws_lambda` as shown following.

```
CREATE EXTENSION IF NOT EXISTS aws_lambda CASCADE;
NOTICE: installing required extension "aws_commons"
CREATE EXTENSION
```

The aws_lambda extension is installed in your DB instance. You can now create convenience structures for invoking your Lambda functions.

Step 4: Use Lambda helper functions with your RDS for PostgreSQL DB instance (Optional)

You can use the helper functions in the aws_commons extension to prepare entities that you can more easily invoke from PostgreSQL. To do this, you need to have the following information about your Lambda functions:

- **Function name** – The name, Amazon Resource Name (ARN), version, or alias of the Lambda function. The IAM policy created in [Step 2: Configure IAM for your instance and Lambda \(p. 1896\)](#) requires the ARN, so we recommend that you use your function's ARN.
- **AWS Region** – (Optional) The AWS Region where the Lambda function is located if it's not in the same Region as your RDS for PostgreSQL DB instance.

To hold the Lambda function name information, you use the [aws_commons.create_lambda_function_arn \(p. 1905\)](#) function. This helper function creates an aws_commons._lambda_function_arn_1 composite structure with the details needed by the invoke function. Following, you can find three alternative approaches to setting up this composite structure.

```
SELECT aws_commons.create_lambda_function_arn(  
    'my-function',  
    'aws-region'  
) AS aws_lambda_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(  
    '111122223333:function:my-function',  
    'aws-region'  
) AS lambda_partial_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(  
    'arn:aws:lambda:aws-region:111122223333:function:my-function'  
) AS lambda_arn_1 \gset
```

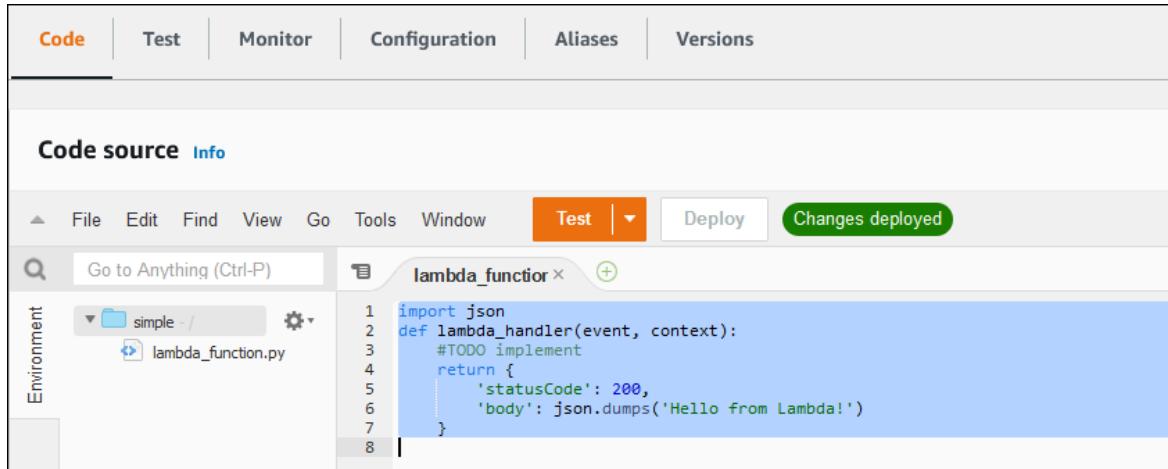
Any of these values can be used in calls to the [aws_lambda.invoke \(p. 1903\)](#) function. For examples, see [Step 5: Invoke a Lambda function from your RDS for PostgreSQL DB instance \(p. 1898\)](#).

Step 5: Invoke a Lambda function from your RDS for PostgreSQL DB instance

The aws_lambda.invoke function behaves synchronously or asynchronously, depending on the invocation_type. The two alternatives for this parameter are RequestResponse (the default) and Event, as follows.

- **RequestResponse** – This invocation type is *synchronous*. It's the default behavior when the call is made without specifying an invocation type. The response payload includes the results of the aws_lambda.invoke function. Use this invocation type when your workflow requires receiving results from the Lambda function before proceeding.
- **Event** – This invocation type is *asynchronous*. The response doesn't include a payload containing results. Use this invocation type when your workflow doesn't need a result from the Lambda function to continue processing.

As a simple test of your setup, you can connect to your DB instance using `psql` and invoke an example function from the command line. Suppose that you have one of the basic functions set up on your Lambda service, such as the simple Python function shown in the following screenshot.



The screenshot shows the AWS Lambda console's "Code source" tab. The "lambda_function" file contains the following Python code:

```

1 import json
2 def lambda_handler(event, context):
3     #TODO implement
4     return {
5         'statusCode': 200,
6         'body': json.dumps('Hello from Lambda!')
7     }
8

```

To invoke an example function

1. Connect to your DB instance using `psql` or pgAdmin.

```
psql -h instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
```

2. Invoke the function using its ARN.

```
SELECT * from
aws_lambda.invoke(aws_commons.create_lambda_function_arn('arn:aws:lambda:aws-
region:444455556666:function:simple', 'us-west-1'), '{"body": "Hello from
Postgres!"}';json );
```

The response looks as follows.

status_code log_result	payload	executed_version
200 {"statusCode": 200, "body": "\"Hello from Lambda!\""} \$LATEST		

(1 row)

If your invocation attempt doesn't succeed, see [Lambda function error messages \(p. 1902\)](#).

Step 6: Grant other users permission to invoke Lambda functions

At this point in the procedures, only you as `rds_superuser` can invoke your Lambda functions. To allow other users to invoke any functions that you create, you need to grant them permission.

To grant others permission to invoke Lambda functions

1. Connect to your DB instance using `psql` or pgAdmin.

```
psql -h instance.44445556666.aws-region.rds.amazonaws.com -U postgres -p 5432
```

- Run the following SQL commands:

```
postgres=> GRANT USAGE ON SCHEMA aws_lambda TO db_username;  
GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA aws_lambda TO db_username;
```

Examples: Invoking Lambda functions from your RDS for PostgreSQL DB instance

Following, you can find several examples of calling the `aws_lambda.invoke` (p. 1903) function. Most all the examples use the composite structure `aws_lambda_arn_1` that you create in [Step 4: Use Lambda helper functions with your RDS for PostgreSQL DB instance \(Optional\)](#) (p. 1898) to simplify passing the function details. For an example of asynchronous invocation, see [Example: Asynchronous \(Event\) invocation of Lambda functions](#) (p. 1901). All the other examples listed use synchronous invocation.

To learn more about Lambda invocation types, see [Invoking Lambda functions](#) in the *AWS Lambda Developer Guide*. For more information about `aws_lambda_arn_1`, see [aws_commons.create_lambda_function_arn](#) (p. 1905).

Examples list

- [Example: Synchronous \(RequestResponse\) invocation of Lambda functions](#) (p. 1900)
- [Example: Asynchronous \(Event\) invocation of Lambda functions](#) (p. 1901)
- [Example: Capturing the Lambda execution log in a function response](#) (p. 1901)
- [Example: Including client context in a Lambda function](#) (p. 1901)
- [Example: Invoking a specific version of a Lambda function](#) (p. 1901)

Example: Synchronous (RequestResponse) invocation of Lambda functions

Following are two examples of a synchronous Lambda function invocation. The results of these `aws_lambda.invoke` function calls are the same.

```
SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"'}::json);
```

```
SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"'}::json, 'RequestResponse');
```

The parameters are described as follows:

- `: 'aws_lambda_arn_1'` – This parameter identifies the composite structure created in [Step 4: Use Lambda helper functions with your RDS for PostgreSQL DB instance \(Optional\)](#) (p. 1898), with the `aws_commons.create_lambda_function_arn` helper function. You can also create this structure inline within your `aws_lambda.invoke` call as follows.

```
SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function',  
'aws-region'),  
'{\"body\": \"Hello from Postgres!\"'}::json
```

```
 );
```

- `'{"body": "Hello from PostgreSQL!"}':json` – The JSON payload to pass to the Lambda function.
- `'RequestResponse'` – The Lambda invocation type.

Example: Asynchronous (Event) invocation of Lambda functions

Following is an example of an asynchronous Lambda function invocation. The Event invocation type schedules the Lambda function invocation with the specified input payload and returns immediately. Use the Event invocation type in certain workflows that don't depend on the results of the Lambda function.

```
SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}':json, 'Event');
```

Example: Capturing the Lambda execution log in a function response

You can include the last 4 KB of the execution log in the function response by using the `log_type` parameter in your `aws_lambda.invoke` function call. By default, this parameter is set to `None`, but you can specify `Tail` to capture the results of the Lambda execution log in the response, as shown following.

```
SELECT *, select convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}':json, 'RequestResponse', 'Tail');
```

Set the [aws_lambda.invoke \(p. 1903\)](#) function's `log_type` parameter to `Tail` to include the execution log in the response. The default value for the `log_type` parameter is `None`.

The `log_result` that's returned is a base64 encoded string. You can decode the contents using a combination of the `decode` and `convert_from` PostgreSQL functions.

For more information about `log_type`, see [aws_lambda.invoke \(p. 1903\)](#).

Example: Including client context in a Lambda function

The `aws_lambda.invoke` function has a `context` parameter that you can use to pass information separate from the payload, as shown following.

```
SELECT *, convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}':json, 'RequestResponse', 'Tail');
```

To include client context, use a JSON object for the [aws_lambda.invoke \(p. 1903\)](#) function's `context` parameter.

For more information about the `context` parameter, see the [aws_lambda.invoke \(p. 1903\)](#) reference.

Example: Invoking a specific version of a Lambda function

You can specify a particular version of a Lambda function by including the `qualifier` parameter with the `aws_lambda.invoke` call. Following, you can find an example that does this using '`custom_version`' as an alias for the version.

```
SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}':json, 'RequestResponse', 'None', NULL, 'custom_version');
```

You can also supply a Lambda function qualifier with the function name details instead, as follows.

```
SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function:custom_version', 'us-west-2'), '{"body": "Hello from Postgres!"}':json);
```

For more information about qualifier and other parameters, see the [aws_lambda.invoke \(p. 1903\)](#) reference.

Lambda function error messages

In the following list you can find information about error messages, with possible causes and solutions.

- **VPC configuration issues**

VPC configuration issues can raise the following error messages when trying to connect:

```
ERROR: invoke API failed
DETAIL: AWS Lambda client returned 'Unable to connect to endpoint'.
CONTEXT: SQL function "invoke" statement 1
```

A common cause for this error is improperly configured VPC security group. Make sure you have an outbound rule for TCP open on port 443 of your VPC security group so that your VPC can connect to the Lambda VPC.

If your DB instance is private, check the private DNS setup for your VPC. Make sure that you set the `rds.custom_dns_resolution` parameter to 1 and setup AWS PrivateLink as outlined in [Step 1: Configure your RDS for PostgreSQL DB instance for outbound connections to AWS Lambda \(p. 1895\)](#). For more information, see [Interface VPC endpoints \(AWS PrivateLink\)](#).

- **Lack of permissions needed to invoke Lambda functions**

If you see either of the following error messages, the user (role) invoking the function doesn't have proper permissions.

```
ERROR: permission denied for schema aws_lambda
```

```
ERROR: permission denied for function invoke
```

A user (role) must be given specific grants to invoke Lambda functions. For more information, see [Step 6: Grant other users permission to invoke Lambda functions \(p. 1899\)](#).

- **Improper handling of errors in your Lambda functions**

If a Lambda function throws an exception during request processing, `aws_lambda.invoke` fails with a PostgreSQL error such as the following.

```
SELECT * FROM aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}':json);
ERROR: lambda invocation failed
DETAIL: "arn:aws:lambda:us-west-2:555555555555:function:my-function" returned error
"Unhandled", details: "<Error details string>".
```

Be sure to handle errors in your Lambda functions or in your PostgreSQL application.

AWS Lambda function reference

Following is the reference for the functions to use for invoking Lambda functions with RDS for PostgreSQL.

Functions

- [aws_lambda.invoke \(p. 1903\)](#)
- [aws_commons.create_lambda_function_arn \(p. 1905\)](#)

aws_lambda.invoke

Runs a Lambda function for an RDS for PostgreSQL DB instance.

For more details about invoking Lambda functions, see also [Invoke](#) in the *AWS Lambda Developer Guide*.

Syntax

JSON

```
aws_lambda.invoke(
    IN function_name TEXT,
    IN payload JSON,
    IN region TEXT DEFAULT NULL,
    IN invocation_type TEXT DEFAULT 'RequestResponse',
    IN log_type TEXT DEFAULT 'None',
    IN context JSON DEFAULT NULL,
    IN qualifier VARCHAR(128) DEFAULT NULL,
    OUT status_code INT,
    OUT payload JSON,
    OUT executed_version TEXT,
    OUT log_result TEXT)
```

```
aws_lambda.invoke(
    IN function_name aws_commons._lambda_function_arn_1,
    IN payload JSON,
    IN invocation_type TEXT DEFAULT 'RequestResponse',
    IN log_type TEXT DEFAULT 'None',
    IN context JSON DEFAULT NULL,
    IN qualifier VARCHAR(128) DEFAULT NULL,
    OUT status_code INT,
    OUT payload JSON,
    OUT executed_version TEXT,
    OUT log_result TEXT)
```

JSONB

```
aws_lambda.invoke(
    IN function_name TEXT,
    IN payload JSONB,
    IN region TEXT DEFAULT NULL,
    IN invocation_type TEXT DEFAULT 'RequestResponse',
    IN log_type TEXT DEFAULT 'None',
    IN context JSONB DEFAULT NULL,
    IN qualifier VARCHAR(128) DEFAULT NULL,
```

```
    OUT status_code INT,
    OUT payload JSONB,
    OUT executed_version TEXT,
    OUT log_result TEXT)
```

```
aws_lambda.invoke(
IN function_name aws_commons._lambda_function_arn_1,
IN payload JSONB,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSONB DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSONB,
OUT executed_version TEXT,
OUT log_result TEXT
)
```

Input parameters

function_name

The identifying name of the Lambda function. The value can be the function name, an ARN, or a partial ARN. For a listing of possible formats, see [Lambda function name formats](#) in the *AWS Lambda Developer Guide*.

payload

The input for the Lambda function. The format can be JSON or JSONB. For more information, see [JSON Types](#) in the PostgreSQL documentation.

region

(Optional) The Lambda Region for the function. By default, RDS resolves the AWS Region from the full ARN in the *function_name* or it uses the RDS for PostgreSQL DB instance Region. If this Region value conflicts with the one provided in the *function_name* ARN, an error is raised.

invocation_type

The invocation type of the Lambda function. The value is case-sensitive. Possible values include the following:

- RequestResponse – The default. This type of invocation for a Lambda function is synchronous and returns a response payload in the result. Use the RequestResponse invocation type when your workflow depends on receiving the Lambda function result immediately.
- Event – This type of invocation for a Lambda function is asynchronous and returns immediately without a returned payload. Use the Event invocation type when you don't need results of the Lambda function before your workflow moves on.
- DryRun – This type of invocation tests access without running the Lambda function.

log_type

The type of Lambda log to return in the *log_result* output parameter. The value is case-sensitive. Possible values include the following:

- Tail – The returned *log_result* output parameter will include the last 4 KB of the execution log.
- None – No Lambda log information is returned.

context

Client context in JSON or JSONB format. Fields to use include `custom` and `env`.

qualifier

A qualifier that identifies a Lambda function's version to be invoked. If this value conflicts with one provided in the `function_name` ARN, an error is raised.

Output parameters

status_code

An HTTP status response code. For more information, see [Lambda Invoke response elements](#) in the [AWS Lambda Developer Guide](#).

payload

The information returned from the Lambda function that ran. The format is in JSON or JSONB.

executed_version

The version of the Lambda function that ran.

log_result

The execution log information returned if the `log_type` value is `Tail` when the Lambda function was invoked. The result contains the last 4 KB of the execution log encoded in Base64.

[aws_commons.create_lambda_function_arn](#)

Creates an `aws_commons._lambda_function_arn_1` structure to hold Lambda function name information. You can use the results of the `aws_commons.create_lambda_function_arn` function in the `function_name` parameter of the `aws_lambda.invoke` ([p. 1903](#)) function.

Syntax

```
aws_commons.create_lambda_function_arn(  
    function_name TEXT,  
    region TEXT DEFAULT NULL  
)  
RETURNS aws_commons._lambda_function_arn_1
```

Input parameters

function_name

A required text string containing the Lambda function name. The value can be a function name, a partial ARN, or a full ARN.

region

An optional text string containing the AWS Region that the Lambda function is in. For a listing of Region names and associated values, see [Regions, Availability Zones, and Local Zones \(p. 72\)](#).

Working with PostgreSQL features supported by Amazon RDS for PostgreSQL

Amazon RDS for PostgreSQL supports many of the most common PostgreSQL features. For example, PostgreSQL has an autovacuum feature that performs routine maintenance on the database. The

autovacuum feature is active by default. Although you can turn off this feature, we highly recommend that you keep it on. Understanding this feature and what you can do to make sure it works as it should is a basic task of any DBA. For more information about the autovacuum, see [Working with the PostgreSQL autovacuum on Amazon RDS for PostgreSQL \(p. 1924\)](#). To learn more about other common DBA tasks, [Common DBA tasks for Amazon RDS for PostgreSQL \(p. 1915\)](#).

RDS for PostgreSQL also supports extensions that add important functionality to the DB instance. For example, you can use the PostGIS extension to work with spatial data, or use the pg_cron extension to schedule maintenance from within the instance. For more information about PostgreSQL extensions, see [Using PostgreSQL extensions with Amazon RDS for PostgreSQL \(p. 1945\)](#).

Foreign data wrappers are a specific type of extension designed to let your RDS for PostgreSQL DB instance work with other commercial databases or data types. For more information about foreign data wrappers supported by RDS for PostgreSQL, see [Working with the supported foreign data wrappers for Amazon RDS for PostgreSQL \(p. 1987\)](#).

Following, you can find information about some other features supported by RDS for PostgreSQL.

Topics

- [Custom data types and enumerations with RDS for PostgreSQL \(p. 1906\)](#)
- [Event triggers for RDS for PostgreSQL \(p. 1907\)](#)
- [Huge pages for RDS for PostgreSQL \(p. 1907\)](#)
- [Performing logical replication for Amazon RDS for PostgreSQL \(p. 1908\)](#)
- [RAM disk for the stats_temp_directory \(p. 1909\)](#)
- [Tablespaces for RDS for PostgreSQL \(p. 1910\)](#)
- [RDS for PostgreSQL collations for EBCDIC and other mainframe migrations \(p. 1910\)](#)

Custom data types and enumerations with RDS for PostgreSQL

PostgreSQL supports creating custom data types and working with enumerations. For more information about creating and working with enumerations and other data types, see [Enumerated types](#) in the PostgreSQL documentation.

The following is an example of creating a type as an enumeration and then inserting values into a table.

```
CREATE TYPE rainbow AS ENUM ('red', 'orange', 'yellow', 'green', 'blue', 'purple');
CREATE TYPE
CREATE TABLE t1 (colors rainbow);
CREATE TABLE
INSERT INTO t1 VALUES ('red'), ('orange');
INSERT 0 2
SELECT * from t1;
colors
-----
red
orange
(2 rows)
postgres=> ALTER TYPE rainbow RENAME VALUE 'red' TO 'crimson';
ALTER TYPE
postgres=> SELECT * from t1;
colors
-----
crimson
orange
(2 rows)
```

Event triggers for RDS for PostgreSQL

All current PostgreSQL versions support event triggers, and so do all available versions of RDS for PostgreSQL. You can use the main user account (default, `postgres`) to create, modify, rename, and delete event triggers. Event triggers are at the DB instance level, so they can apply to all databases on an instance.

For example, the following code creates an event trigger that prints the current user at the end of every data definition language (DDL) command.

```
CREATE OR REPLACE FUNCTION raise_notice_func()
RETURNS event_trigger
LANGUAGE plpgsql AS
$$
BEGIN
    RAISE NOTICE 'In trigger function: %', current_user;
END;
$$;

CREATE EVENT TRIGGER event_trigger_1
ON ddl_command_end
EXECUTE PROCEDURE raise_notice_func();
```

For more information about PostgreSQL event triggers, see [Event triggers](#) in the PostgreSQL documentation.

There are several limitations to using PostgreSQL event triggers on Amazon RDS. These include the following:

- You can't create event triggers on read replicas. You can, however, create event triggers on a read replica source. The event triggers are then copied to the read replica. The event triggers on the read replica don't fire on the read replica when changes are pushed from the source. However, if the read replica is promoted, the existing event triggers fire when database operations occur.
- To perform a major version upgrade to a PostgreSQL DB instance that uses event triggers, make sure to delete the event triggers before you upgrade the instance.

Huge pages for RDS for PostgreSQL

Huge pages are a memory management feature that reduces overhead when a DB instance is working with large contiguous chunks of memory, such as that used by shared buffers. This PostgreSQL feature is supported by all currently available RDS for PostgreSQL versions. You allocate huge pages for your application by using calls to `mmap` or `SYSV` shared memory. RDS for PostgreSQL supports both 4-KB and 2-MB page sizes.

You can turn huge pages on or off by changing the value of the `huge_pages` parameter. The feature is turned on by default for all DB instance classes other than micro, small, and medium DB instance classes.

Note

Huge pages aren't supported for `db.m1`, `db.m2`, and `db.m3` DB instance classes.

RDS for PostgreSQL uses huge pages based on the available shared memory. If the DB instance can't use huge pages due to shared memory constraints, Amazon RDS prevents the DB instance from starting. In this case, Amazon RDS sets the status of the DB instance to an incompatible parameters state. If this occurs, you can set the `huge_pages` parameter to `off` to allow Amazon RDS to start the DB instance.

The `shared_buffers` parameter is key to setting the shared memory pool that is required for using huge pages. The default value for the `shared_buffers` parameter uses a database parameters macro.

This macro sets a percentage of the total 8 KB pages available for the DB instance's memory. When you use huge pages, those pages are located with the huge pages. Amazon RDS puts a DB instance into an incompatible parameters state if the shared memory parameters are set to require more than 90 percent of the DB instance memory.

To learn more about PostgreSQL memory management, see [Resource Consumption](#) in the PostgreSQL documentation.

Performing logical replication for Amazon RDS for PostgreSQL

Starting with version 10.4, RDS for PostgreSQL supports the publication and subscription SQL syntax that was introduced in PostgreSQL 10. To learn more, see [Logical replication](#) in the PostgreSQL documentation.

Note

In addition to the native PostgreSQL logical replication feature introduced in PostgreSQL 10, RDS for PostgreSQL also supports the pglogical extension. For more information, see [Using pglogical to synchronize data across instances \(p. 1967\)](#).

Following, you can find information about setting up logical replication for an RDS for PostgreSQL DB instance.

Topics

- [Understanding logical replication and logical decoding \(p. 1908\)](#)
- [Working with logical replication slots \(p. 1909\)](#)

Understanding logical replication and logical decoding

RDS for PostgreSQL supports the streaming of write-ahead log (WAL) changes using PostgreSQL's logical replication slots. It also supports using logical decoding. You can set up logical replication slots on your instance and stream database changes through these slots to a client such as `pg_recvlogical`. You create logical replication slots at the database level, and they support replication connections to a single database.

The most common clients for PostgreSQL logical replication are AWS Database Migration Service or a custom-managed host on an Amazon EC2 instance. The logical replication slot has no information about the receiver of the stream. Also, there's no requirement that the target be a replica database. If you set up a logical replication slot and don't read from the slot, data can be written and quickly fill up your DB instance's storage.

You turn on PostgreSQL logical replication and logical decoding for Amazon RDS with a parameter, a replication connection type, and a security role. The client for logical decoding can be any client that can establish a replication connection to a database on a PostgreSQL DB instance.

To turn on logical decoding for an RDS for PostgreSQL DB instance

1. Make sure that the user account that you're using has these roles:
 - The `rds_superuser` role so you can turn on logical replication
 - The `rds_replication` role to grant permissions to manage logical slots and to stream data using logical slots
2. Set the `rds.logical_replication` static parameter to 1. As part of applying this parameter, also set the parameters `wal_level`, `max_wal_senders`, `max_replication_slots`, and `max_connections`. These parameter changes can increase WAL generation, so set the `rds.logical_replication` parameter only when you are using logical slots.

3. Reboot the DB instance for the static `rds.logical_replication` parameter to take effect.
4. Create a logical replication slot as explained in the next section. This process requires that you specify a decoding plugin. Currently, RDS for PostgreSQL supports the `test_decoding` and `wal2json` output plugins that ship with PostgreSQL.

For more information on PostgreSQL logical decoding, see the [PostgreSQL documentation](#).

Working with logical replication slots

You can use SQL commands to work with logical slots. For example, the following command creates a logical slot named `test_slot` using the default PostgreSQL output plugin `test_decoding`.

```
SELECT * FROM pg_create_logical_replication_slot('test_slot', 'test_decoding');
slot_name | xlog_position
-----+-----
regression_slot | 0/16B1970
(1 row)
```

To list logical slots, use the following command.

```
SELECT * FROM pg_replication_slots;
```

To drop a logical slot, use the following command.

```
SELECT pg_drop_replication_slot('test_slot');
pg_drop_replication_slot
-----+
(1 row)
```

For more examples on working with logical replication slots, see [Logical decoding examples](#) in the PostgreSQL documentation.

After you create the logical replication slot, you can start streaming. The following example shows how logical decoding is controlled over the streaming replication protocol. This example uses the program `pg_recvlogical`, which is included in the PostgreSQL distribution. Doing this requires that client authentication is set up to allow replication connections.

```
pg_recvlogical -d postgres --slot test_slot -U postgres
  --host -i<instance-name>.111122223333.aws-region.rds.amazonaws.com
  -f - --start
```

To see the contents of the `pg_replication_origin_status` view, query the `pg_show_replication_origin_status` function.

```
SELECT * FROM pg_show_replication_origin_status();
local_id | external_id | remote_lsn | local_lsn
-----+-----+-----+-----+
(0 rows)
```

RAM disk for the stats_temp_directory

You can use the RDS for PostgreSQL parameter `rds.pg_stat_ramdisk_size` to specify the system memory allocated to a RAM disk for storing the PostgreSQL `stats_temp_directory`. The RAM disk parameter is available for all PostgreSQL versions on Amazon RDS.

Under certain workloads, setting this parameter can improve performance and decrease I/O requirements. For more information about the `stats_temp_directory`, see [the PostgreSQL documentation](#).

To set up a RAM disk for your `stats_temp_directory`, set the `rds.pg_stat_ramdisk_size` parameter to an integer literal value in the parameter group used by your DB instance. This parameter denotes MB, so you must use an integer value. Expressions, formulas, and functions aren't valid for the `rds.pg_stat_ramdisk_size` parameter. Be sure to reboot the DB instance so that the change takes effect. For information about setting parameters, see [Working with parameter groups \(p. 289\)](#).

For example, the following AWS CLI command sets the RAM disk parameter to 256 MB.

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name pg-95-ramdisk-testing \
  --parameters "ParameterName=rds.pg_stat_ramdisk_size, ParameterValue=256,
  ApplyMethod=pending-reboot"
```

After you reboot, run the following command to see the status of the `stats_temp_directory`.

```
postgres=> SHOW stats_temp_directory;
```

The command should return the following.

```
stats_temp_directory
-----
/rdsdbramdisk/pg_stat_tmp
(1 row)
```

Tablespaces for RDS for PostgreSQL

RDS for PostgreSQL supports tablespaces for compatibility. Because all storage is on a single logical volume, you can't use tablespaces for I/O splitting or isolation. Our benchmarks and experience indicate that a single logical volume is the best setup for most use cases.

To create and use tablespaces with your RDS for PostgreSQL DB instance requires the `rds_superuser` role. Your RDS for PostgreSQL DB instance's main user account (default name, `postgres`) is a member of this role. For more information, see [Understanding PostgreSQL roles and permissions \(p. 1915\)](#).

If you specify a file name when you create a tablespace, the path prefix is `/rdsdbdata/db/base/tablespace`. The following example places tablespace files in `/rdsdbdata/db/base/tablespace/data`. This example assumes that a `dbadmin` user (role) exists and that it's been granted the `rds_superuser` role needed to work with tablespaces.

```
postgres=> CREATE TABLESPACE act_data
  OWNER dbadmin
  LOCATION '/data';
CREATE TABLESPACE
```

To learn more about PostgreSQL tablespaces, see [Tablespaces in the PostgreSQL documentation](#).

RDS for PostgreSQL collations for EBCDIC and other mainframe migrations

RDS for PostgreSQL versions 10 and higher include ICU version 60.2, which is based on Unicode 10.0 and includes collations from the Unicode Common Locale Data Repository, CLDR 32. These software

internationalization libraries ensure that character encodings are presented in a consistent way, regardless of operating system or platform. For more information about Unicode CLDR-32, see the [CLDR 32 Release Note](#) on the Unicode CLDR website. You can learn more about the internationalization components for Unicode (ICU) at the [ICU Technical Committee \(ICU-TC\)](#) website. For information about ICU-60, see [Download ICU 60](#).

Starting with version 14.3, RDS for PostgreSQL also includes collations that help with data integration and conversion from EBCDIC-based systems. The extended binary coded decimal interchange code or *EBCDIC* encoding is commonly used by mainframe operating systems. These Amazon RDS-provided collations are narrowly defined to sort only those Unicode characters that directly map to EBCDIC code pages. The characters are sorted in EBCDIC code-point order to allow for data validation after conversion. These collations don't include denormalized forms, nor do they include Unicode characters that don't directly map to a character on the source EBCDIC code page.

The character mappings between EBCDIC code pages and Unicode code points are based on tables published by IBM. The complete set is available from IBM as a [compressed file](#) for download. RDS for PostgreSQL used these mappings with tools provided by the ICU to create the collations listed in the tables in this section. The collation names include a language and country as required by the ICU. However, EBCDIC code pages don't specify languages, and some EBCDIC code pages cover multiple countries. That means that the language and country portion of the collation names in the table are arbitrary, and they don't need to match the current locale. In other words, the code page number is the most important part of the collation name in this table. You can use any of the collations listed in the following tables in any RDS for PostgreSQL database.

- [Unicode to EBCDIC collations table](#) – Some mainframe data migration tools internally use LATIN1 or LATIN9 to encode and process data. Such tools use round-trip schemes to preserve data integrity and support reverse conversion. The collations in this table can be used by tools that process data using LATIN1 encoding, which doesn't require special handling.
- [Unicode to LATIN9 collations table](#) – You can use these collations in any RDS for PostgreSQL database.

In the following table, you find collations available in RDS for PostgreSQL that map EBCDIC code pages to Unicode code points. We recommend that you use the collations in this table for application development that requires sorting based on the ordering of IBM code pages.

PostgreSQL collation name	Description of code-page mapping and sort order
da-DK-cp277-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 277 (per conversion tables) are sorted in IBM CP 277 code point order
de-DE-cp273-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 273 (per conversion tables) are sorted in IBM CP 273 code point order
en-GB-cp285-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 285 (per conversion tables) are sorted in IBM CP 285 code point order
en-US-cp037-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 037 (per conversion tables) are sorted in IBM CP 37 code point order
es-ES-cp284-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 284 (per conversion tables) are sorted in IBM CP 284 code point order

PostgreSQL collation name	Description of code-page mapping and sort order
fi-FI-cp278-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 278 (per conversion tables) are sorted in IBM CP 278 code point order
fr-FR-cp297-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 297 (per conversion tables) are sorted in IBM CP 297 code point order
it-IT-cp280-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 280 (per conversion tables) are sorted in IBM CP 280 code point order
nl-BE-cp500-x-icu	Unicode characters that directly map to IBM EBCDIC Code Page 500 (per conversion tables) are sorted in IBM CP 500 code point order

Amazon RDS provides a set of additional collations that sort Unicode code points that map to LATIN9 characters using the tables published by IBM, in the order of the original code points according to the EBCDIC code page of the source data.

PostgreSQL collation name	Description of code-page mapping and sort order
da-DK-cp1142m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1142 (per conversion tables) are sorted in IBM CP 1142 code point order
de-DE-cp1141m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1141 (per conversion tables) are sorted in IBM CP 1141 code point order
en-GB-cp1146m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1146 (per conversion tables) are sorted in IBM CP 1146 code point order
en-US-cp1140m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1140 (per conversion tables) are sorted in IBM CP 1140 code point order
es-ES-cp1145m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1145 (per conversion tables) are sorted in IBM CP 1145 code point order
fi-FI-cp1143m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1143 (per conversion tables) are sorted in IBM CP 1143 code point order
fr-FR-cp1147m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page

PostgreSQL collation name	Description of code-page mapping and sort order
	1147 (per conversion tables) are sorted in IBM CP 1147 code point order
it-IT-cp1144m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1144 (per conversion tables) are sorted in IBM CP 1144 code point order
nl-BE-cp1148m-x-icu	Unicode characters that map to LATIN9 characters originally converted from IBM EBCDIC Code Page 1148 (per conversion tables) are sorted in IBM CP 1148 code point order

In the following, you can find an example of using an RDS for PostgreSQL collation.

```
db1=> SELECT pg_import_system_collations('pg_catalog');
 pg_import_system_collations
-----
      36
db1=> SELECT '¤' < 'a' col1;
 col1
-----
      t
db1=> SELECT '¤' < 'a' COLLATE "da-DK-cp277-x-icu" col1;
 col1
-----
      f
```

We recommend that you use the collations in the [Unicode to EBCDIC collations table](#) and in the [Unicode to LATIN9 collations table](#) for application development that requires sorting based on the ordering of IBM code pages. The following collations (suffixed with the letter “b”) are also visible in pg_collation, but are intended for use by mainframe data integration and migration tools at AWS that map code pages with specific code point shifts and require special handling in collation. In other words, the following collations aren’t recommended for use.

- da-DK-277b-x-icu
- da-DK-1142b-x-icu
- de-DE-cp273b-x-icu
- de-DE-cp1141b-x-icu
- en-GB-cp1146b-x-icu
- en-GB-cp285b-x-icu
- en-US-cp037b-x-icu
- en-US-cp1140b-x-icu
- es-ES-cp1145b-x-icu
- es-ES-cp284b-x-icu
- fi-FI-cp1143b-x-icu
- fr-FR-cp1147b-x-icu
- fr-FR-cp297b-x-icu
- it-IT-cp1144b-x-icu
- it-IT-cp280b-x-icu
- nl-BE-cp1148b-x-icu

- nl-BE-cp500b-x-icu

To learn more about migrating applications from mainframe environments to AWS, see [What is AWS Mainframe Modernization?](#).

For more information about managing collations in PostgreSQL, see [Collation Support](#) in the PostgreSQL documentation.

Common DBA tasks for Amazon RDS for PostgreSQL

Database administrators (DBAs) perform a variety of tasks when administering an Amazon RDS for PostgreSQL DB instance. If you're a DBA already familiar with PostgreSQL, you need to be aware of some of the important differences between running PostgreSQL on your hardware and RDS for PostgreSQL. For example, because it's a managed service, Amazon RDS doesn't allow shell access to your DB instances. That means that you don't have direct access to `pg_hba.conf` and other configuration files. For RDS for PostgreSQL, changes that are typically made to the PostgreSQL configuration file of an on-premises instance are made to a custom DB parameter group associated with the RDS for PostgreSQL DB instance. For more information, see [Working with parameter groups \(p. 289\)](#).

You also can't access log files in the same way that you do with an on-premises PostgreSQL instance. To learn more about logging, see [RDS for PostgreSQL database log files \(p. 716\)](#).

As another example, you don't have access to the PostgreSQL superuser account. On RDS for PostgreSQL, the `rds_superuser` role is the most highly privileged role, and it's granted to `postgres` at set up time. Whether you're familiar with using PostgreSQL on-premises or completely new to RDS for PostgreSQL, we recommend that you understand the `rds_superuser` role, and how to work with roles, users, groups, and permissions. For more information, see [Understanding PostgreSQL roles and permissions \(p. 1915\)](#).

Following are some common DBA tasks for RDS for PostgreSQL.

Topics

- [Understanding PostgreSQL roles and permissions \(p. 1915\)](#)
- [Working with the PostgreSQL autovacuum on Amazon RDS for PostgreSQL \(p. 1924\)](#)
- [Working with logging mechanisms supported by RDS for PostgreSQL \(p. 1933\)](#)
- [Using pgBadger for log analysis with PostgreSQL \(p. 1933\)](#)
- [Working with parameters on your RDS for PostgreSQL DB instance \(p. 1934\)](#)

Understanding PostgreSQL roles and permissions

When you create an RDS for PostgreSQL DB instance using the AWS Management Console, an administrator account is created at the same time. By default, its name is `postgres`, as shown in the following screenshot:

The screenshot shows the 'Credentials Settings' section of the AWS Management Console. It includes fields for 'Master username' (set to 'postgres'), 'Master password' (a masked password), and 'Confirm password' (a masked password). There are also options for 'Auto generate a password' and 'Constraints' regarding password length and characters.

▼ Credentials Settings	
Master username	Info Type a login ID for the master user of your DB instance. <input type="text" value="postgres"/>
1 to 16 alphanumeric characters. First character must be a letter.	
<input type="checkbox"/> Auto generate a password	Amazon RDS can generate a password for you, or you can specify your own password.
Master password	Info <input type="password" value="*****"/> Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), '(single quote), "(double quote) and @ (at sign).
Confirm password	Info <input type="password" value="*****"/>

You can choose another name rather than accept the default (`postgres`). If you do, the name you choose must start with a letter and be between 1 and 16 alphanumeric characters. For simplicity's sake, we refer to this main user account by its default value (`postgres`) throughout this guide.

If you use the `create-db-instance` AWS CLI rather than the AWS Management Console, you create the name by passing it with the `master-username` parameter in the command. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

Whether you use the AWS Management Console, the AWS CLI, or the Amazon RDS API, and whether you use the default `postgres` name or choose a different name, this first database user account is a member of the `rds_superuser` group and has `rds_superuser` privileges.

Topics

- [Understanding the rds_superuser role \(p. 1916\)](#)
- [Controlling user access to the PostgreSQL database \(p. 1917\)](#)
- [Delegating and controlling user password management \(p. 1919\)](#)
- [Using SCRAM for PostgreSQL password encryption \(p. 1920\)](#)

Understanding the `rds_superuser` role

In PostgreSQL, a *role* can define a user, a group, or a set of specific permissions granted to a group or user for various objects in the database. PostgreSQL commands to `CREATE USER` and `CREATE GROUP` have been replaced by the more general, `CREATE ROLE` with specific properties to distinguish database users. A database user can be thought of as a role with the `LOGIN` privilege.

Note

The `CREATE USER` and `CREATE GROUP` commands can still be used. For more information, see [Database Roles](#) in the PostgreSQL documentation.

The `postgres` user is the most highly privileged database user on your RDS for PostgreSQL DB instance. It has the characteristics defined by the following `CREATE ROLE` statement.

```
CREATE ROLE postgres WITH LOGIN NOSUPERUSER INHERIT CREATEDB CREATEROLE NOREPLICATION VALID UNTIL 'infinity'
```

The properties `NOSUPERUSER`, `NOREPLICATION`, `INHERIT`, and `VALID UNTIL 'infinity'` are the default options for `CREATE ROLE`, unless otherwise specified.

By default, `postgres` has privileges granted to the `rds_superuser` role. The `rds_superuser` role allows the `postgres` user to do the following:

- Add extensions that are available for use with Amazon RDS. For more information, see [Working with PostgreSQL features supported by Amazon RDS for PostgreSQL \(p. 1905\)](#)
- Create roles for users and grant privileges to users. For more information, see `CREATE ROLE` and `GRANT` in the PostgreSQL documentation.
- Create databases. For more information, see `CREATE DATABASE` in the PostgreSQL documentation.
- Grant `rds_superuser` privileges to user roles that don't have these privileges, and revoke privileges as needed. We recommend that you grant this role only to those users who perform superuser tasks. In other words, you can grant this role to database administrators (DBAs) or system administrators.
- Grant (and revoke) the `rds_replication` role to database users that don't have the `rds_superuser` role.
- Grant (and revoke) the `rds_password` role to database users that don't have the `rds_superuser` role.

- Obtain status information about all database connections by using the `pg_stat_activity` view. When needed, `rds_superuser` can stop any connections by using `pg_terminate_backend` or `pg_cancel_backend`.

In the `CREATE ROLE postgres...` statement, you can see that the `postgres` user role specifically disallows PostgreSQL `superuser` permissions. RDS for PostgreSQL is a managed service, so you can't access the host OS, and you can't connect using the PostgreSQL `superuser` account. Many of the tasks that require `superuser` access on a stand-alone PostgreSQL are managed automatically by Amazon RDS.

For more information about granting privileges, see [GRANT](#) in the PostgreSQL documentation.

The `rds_superuser` role is one of several *predefined* roles in an RDS for PostgreSQL DB instance.

Note

In PostgreSQL 13 and earlier releases, *predefined* roles are known as *default* roles.

In the following list, you find some of the other predefined roles that are created automatically for a new RDS for PostgreSQL DB instance. Predefined roles and their privileges can't be changed. You can't drop, rename, or modify privileges for these predefined roles. Attempting to do so results in an error.

- **rds_password** – A role that can change passwords and set up password constraints for database users. The `rds_superuser` role is granted this role by default, and can grant the role to database users. For more information, see [Controlling user access to the PostgreSQL database \(p. 1917\)](#).
- **rdsadmin** – A role that's created to handle many of the management tasks that the administrator with `superuser` privileges would perform on a standalone PostgreSQL database. This role is used internally by RDS for PostgreSQL for many management tasks.
- **rdstopmgr** – A role that's used internally by Amazon RDS to support Multi-AZ deployments.

To see all predefined roles, you can connect to your RDS for PostgreSQL DB instance and use the `psql \du` metacommand. The output looks as follows:

Role name	Attributes	Member of
<code>postgres</code>	<code>Create role, Create DB</code> <code>Password valid until infinity</code>	+ { <code>rds_superuser</code> }
<code>rds_superuser</code>	<code>Cannot login</code>	{ <code>pg_monitor,pg_signal_backend,</code> + <code>rds_replication,rds_password</code> }
...		

In the output, you can see that `rds_superuser` isn't a database user role (it can't login), but it has the privileges of many other roles. You can also see that database user `postgres` is a member of the `rds_superuser` role. As mentioned previously, `postgres` is the default value in the Amazon RDS console's **Create database** page. If you chose another name, that name is shown in the list of roles instead.

Controlling user access to the PostgreSQL database

New databases in PostgreSQL are always created with a default set of privileges in the database's `public` schema that allow all database users and roles to create objects. These privileges allow database users to connect to the database, for example, and create temporary tables while connected.

To better control user access to the databases instances that you create on your RDS for PostgreSQL DB instance, we recommend that you revoke these default public privileges. After doing so, you then grant specific privileges for database users on a more granular basis, as shown in the following procedure.

To set up roles and privileges for a new database instance

Suppose you're setting up a database on a newly created RDS for PostgreSQL DB instance for use by several researchers, all of whom need read-write access to the database.

1. Use psql (or pgAdmin) to connect to your RDS for PostgreSQL DB instance:

```
psql --host=your-db-instance.666666666666.aws-region.rds.amazonaws.com --port=5432 --  
username=postgres --password
```

When prompted, enter your password. The psql client connects and displays the default administrative connection database, `postgres=>`, as the prompt.

2. To prevent database users from creating objects in the public schema, do the following:

```
postgres=> REVOKE CREATE ON SCHEMA public FROM PUBLIC;  
REVOKE
```

3. Next, you create a new database instance:

```
postgres=> CREATE DATABASE lab_db;  
CREATE DATABASE
```

4. Revoke all privileges from the PUBLIC schema on this new database.

```
postgres=> REVOKE ALL ON DATABASE lab_db FROM public;  
REVOKE
```

5. Create a role for database users.

```
postgres=> CREATE ROLE lab_tech;  
CREATE ROLE
```

6. Give database users that have this role the ability to connect to the database.

```
postgres=> GRANT CONNECT ON DATABASE lab_db TO lab_tech;  
GRANT
```

7. Grant all users with the lab_tech role all privileges on this database.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_db TO lab_tech;  
GRANT
```

8. Create database users, as follows:

```
postgres=> CREATE ROLE lab_user1 LOGIN PASSWORD 'change_me';  
CREATE ROLE  
postgres=> CREATE ROLE lab_user2 LOGIN PASSWORD 'change_me';  
CREATE ROLE
```

9. Grant these two users the privileges associated with the lab_tech role:

```
postgres=> GRANT lab_tech TO lab_user1;  
GRANT ROLE  
postgres=> GRANT lab_tech TO lab_user2;  
GRANT ROLE
```

At this point, `lab_user1` and `lab_user2` can connect to the `lab_db` database. This example doesn't follow best practices for enterprise usage, which might include creating multiple database instances, different schemas, and granting limited permissions. For more complete information and additional scenarios, see [Managing PostgreSQL Users and Roles](#).

For more information about privileges in PostgreSQL databases, see the `GRANT` command in the PostgreSQL documentation.

Delegating and controlling user password management

As a DBA, you might want to delegate the management of user passwords. Or, you might want to prevent database users from changing their passwords or reconfiguring password constraints, such as password lifetime. To ensure that only the database users that you choose can change password settings, you can turn on the restricted password management feature. When you activate this feature, only those database users that have been granted the `rds_password` role can manage passwords.

Note

To use restricted password management, your RDS for PostgreSQL DB instance must be running PostgreSQL 10.6 or higher.

By default, this feature is off, as shown in the following:

```
postgres=> SHOW rds.restrict_password_commands;
rds.restrict_password_commands
-----
off
(1 row)
```

To turn on this feature, you use a custom parameter group and change the setting for `rds.restrict_password_commands` to 1. Be sure to reboot your RDS for PostgreSQL DB instance so that the setting takes effect.

With this feature active, `rds_password` privileges are needed for the following SQL commands:

```
CREATE ROLE myrole WITH PASSWORD 'mypassword';
CREATE ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword';
ALTER ROLE myrole VALID UNTIL '2023-01-01';
ALTER ROLE myrole RENAME TO myrole2;
```

Renaming a role (`ALTER ROLE myrole RENAME TO newname`) is also restricted if the password uses the MD5 hashing algorithm.

With this feature active, attempting any of these SQL commands without the `rds_password` role permissions generates the following error:

```
ERROR: must be a member of rds_password to alter passwords
```

We recommend that you grant the `rds_password` to only a few roles that you use solely for password management. If you grant `rds_password` privileges to database users that don't have `rds_superuser` privileges, you need to also grant them the `CREATEROLE` attribute.

Make sure that you verify password requirements such as expiration and needed complexity on the client side. If you use your own client-side utility for password related changes, the utility needs to be a member of `rds_password` and have `CREATE ROLE` privileges.

Using SCRAM for PostgreSQL password encryption

The *Salted Challenge Response Authentication Mechanism (SCRAM)* is an alternative to PostgreSQL's default message digest (MD5) algorithm for encrypting passwords. The SCRAM authentication mechanism is considered more secure than MD5. To learn more about these two different approaches to securing passwords, see [Password Authentication](#) in the PostgreSQL documentation.

We recommend that you use SCRAM rather than MD5 as the password encryption scheme for your RDS for PostgreSQL DB instance. It's a cryptographic challenge-response mechanism that uses the `scram-sha-256` algorithm for password authentication and encryption.

You might need to update libraries for your client applications to support SCRAM. For example, JDBC versions before 42.2.0 don't support SCRAM. For more information, see [PostgreSQL JDBC Driver](#) in the PostgreSQL JDBC Driver documentation. For a list of other PostgreSQL drivers and SCRAM support, see [List of drivers](#) in the PostgreSQL documentation.

Note

RDS for PostgreSQL version 13.1 and higher support `scram-sha-256`. These versions also let you configure your DB instance to require SCRAM, as discussed in the following procedures.

Setting up RDS for PostgreSQL DB instance to require SCRAM

you can require the RDS for PostgreSQL DB instance to accept only passwords that use the `scram-sha-256` algorithm.

Before making changes to your system, be sure you understand the complete process, as follows:

- Get information about all roles and password encryption for all database users.
- Double-check the parameter settings for your RDS for PostgreSQL DB instance for the parameters that control password encryption.
- If your RDS for PostgreSQL DB instance uses a default parameter group, you need to create a custom DB parameter group and apply it to your RDS for PostgreSQL DB instance so that you can modify parameters when needed. If your RDS for PostgreSQL DB instance uses a custom parameter group, you can modify the necessary parameters later in the process, as needed.
- Change the `password_encryption` parameter to `scram-sha-256`.
- Notify all database users that they need to update their passwords. Do the same for your `postgres` account. The new passwords are encrypted and stored using the `scram-sha-256` algorithm.
- Verify that all passwords are encrypted using as the type of encryption.
- If all passwords use `scram-sha-256`, you can change the `rds.accepted_password_auth_method` parameter from `md5+scram` to `scram-sha-256`.

Warning

After you change `rds.accepted_password_auth_method` to `scram-sha-256` alone, any users (roles) with `md5`-encrypted passwords can't connect.

Getting ready to require SCRAM for your RDS for PostgreSQL DB instance

Before making any changes to your RDS for PostgreSQL DB instance, check all existing database user accounts. Also, check the type of encryption used for passwords. You can do these tasks by using the `rds_tools` extension. This extension is supported on RDS for PostgreSQL 13.1 and higher releases.

To get a list of database users (roles) and password encryption methods

1. Use `psql` to connect to your RDS for PostgreSQL DB instance, as shown in the following.

```
psql --host=db-name.111122223333.aws-region.rds.amazonaws.com --port=5432 --  
username=postgres --password
```

2. Install the rds_tools extension.

```
postgres=> CREATE EXTENSION rds_tools;  
CREATE EXTENSION
```

3. Get a listing of roles and encryption.

```
postgres=> SELECT * FROM  
    rds_tools.role_password_encryption_type();
```

You see output similar to the following.

rolname	encryption_type
pg_monitor	
pg_read_all_settings	
pg_read_all_stats	
pg_stat_scan_tables	
pg_signal_backend	
lab_tester	md5
user_465	md5
postgres	md5
(8 rows)	

Creating a custom DB parameter group

Note

If your RDS for PostgreSQL DB instance already uses a custom parameter group, you don't need to create a new one.

For an overview of parameter groups for Amazon RDS, see [Working with parameters on your RDS for PostgreSQL DB instance \(p. 1934\)](#).

The password encryption type used for passwords is set in one parameter, `password_encryption`. The encryption that the RDS for PostgreSQL DB instance allows is set in another parameter, `rds.accepted_password_auth_method`. Changing either of these from the default values requires that you create a custom DB parameter group and apply it to your instance.

You can also use the AWS Management Console or the RDS API to create a custom DB parameter group. For more information, see

You can now associate the custom parameter group with your DB instance.

To create a custom DB parameter group

1. Use the `create-db-parameter-group` CLI command to create the custom DB parameter group. This example uses `postgres13` as the source for this custom parameter group.

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group --db-parameter-group-name 'docs-lab-scram-passwords'  
\  
  --db-parameter-group-family postgres13 --description 'Custom parameter group for  
SCRAM'
```

For Windows:

```
aws rds create-db-parameter-group --db-parameter-group-name "docs-lab-scram-passwords"
^
--db-parameter-group-family postgres13 --description "Custom DB parameter group for
SCRAM"
```

2. Use the [modify-db-instance](#) CLI command to apply this custom parameter group to your RDS for PostgreSQL DB cluster.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance --db-instance-identifier 'your-instance-name' \
--db-parameter-group-name "docs-lab-scram-passwords"
```

For Windows:

```
aws rds modify-db-instance --db-instance-identifier "your-instance-name" ^
--db-parameter-group-name "docs-lab-scram-passwords"
```

To resynchronize your RDS for PostgreSQL DB instance with your custom DB parameter group, you need to reboot the primary and all other instances of the cluster. To minimize impact to your users, schedule this to occur during your regular maintenance window.

Configuring password encryption to use SCRAM

The password encryption mechanism used by an RDS for PostgreSQL DB instance is set in the DB parameter group in the `password_encryption` parameter. Allowed values are `unset`, `md5`, or `scram-sha-256`. The default value depends on the RDS for PostgreSQL version, as follows:

- RDS for PostgreSQL 14 – No default value (`unset`)
- RDS for PostgreSQL 13 – Default is `md5`

With a custom DB parameter group attached to your RDS for PostgreSQL DB instance, you can modify values for the password encryption parameter.

<input type="checkbox"/>	Name	Values	Allowed values	Modifiable	Source	Apply type
<input type="checkbox"/>	<code>password_encryption</code>	<code>md5</code>	<code>md5,scram-sha-256</code>	true	system	dynamic
<input type="checkbox"/>	<code>rds.accepted_password_auth_method</code>	<code>md5+scram</code>	<code>md5+scram, scram</code>	true	system	dynamic

To change password encryption setting to `scram-sha-256`

- Change the value of `password_encryption` to `scram-sha-256`, as shown following. The change can be applied immediately because the parameter is dynamic, so a restart isn't required for the change to take effect.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group --db-parameter-group-name \
'docs-lab-scram-passwords' --parameters
'ParameterName=password_encryption,ParameterValue=scram-sha-256,ApplyMethod=immediate'
```

For Windows:

```
aws rds modify-db-parameter-group --db-parameter-group-name ^
"docs-lab-scram-passwords" --parameters
"ParameterName=password_encryption,ParameterValue=scram-sha-256,ApplyMethod=immediate"
```

Migrating passwords for user roles to SCRAM

You can migrate passwords for user roles to SCRAM as described following.

To migrate database user (role) passwords from MD5 to SCRAM

1. Log in as the administrator user (default user name, `postgres`) as shown following.

```
psql --host=db-name.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password
```

2. Check the setting of the `password_encryption` parameter on your RDS for PostgreSQL DB instance by using the following command.

```
postgres=> SHOW password_encryption;
password_encryption
-----
md5
(1 row)
```

3. Change the value of this parameter to `scram-sha-256`. This is a dynamic parameter, so you don't need to reboot the instance after making this change. Check the value again to make sure that it's now set to `scram-sha-256`, as follows.

```
postgres=> SHOW password_encryption;
password_encryption
-----
scram-sha-256
(1 row)
```

4. Notify all database users to change their passwords. Be sure to also change your own password for account `postgres` (the database user with `rds_superuser` privileges).

```
labdb=> ALTER ROLE postgres WITH LOGIN PASSWORD 'change_me';
ALTER ROLE
```

5. Repeat the process for all databases on your RDS for PostgreSQL DB instance.

Changing parameter to require SCRAM

This is the final step in the process. After you make the change in the following procedure, any user accounts (roles) that still use md5 encryption for passwords can't log in to the RDS for PostgreSQL DB instance.

The `rds.accepted_password_auth_method` specifies the encryption method that the RDS for PostgreSQL DB instance accepts for a user password during the login process. The default value is `md5+scram`, meaning that either method is accepted. In the following image, you can find the default setting for this parameter.

Name	Values	Allowed values	Modifiable	Source	Apply type
password_encryption	scram-sha-256	md5, scram-sha-256	true	system	dynamic
rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic

The allowed values for this parameter are md5+scram or scram alone. Changing this parameter value to scram makes this a requirement.

To change the parameter value to require SCRAM authentication for passwords

- Verify that all database user passwords for all databases on your RDS for PostgreSQL DB instance use scram-sha-256 for password encryption. To do so, query rds_tools for the role (user) and encryption type, as follows.

```
postgres=> SELECT * FROM rds_tools.role_password_encryption_type();
   rolname    | encryption_type
-----+-----
 pg_monitor  |
 pg_read_all_settings |
 pg_read_all_stats  |
 pg_stat_scan_tables |
 pg_signal_backend  |
 lab_tester      | scram-sha-256
 user_465        | scram-sha-256
 postgres         | scram-sha-256
( rows)
```

- Repeat the query across all DB instances in your RDS for PostgreSQL DB instance.

If all passwords use scram-sha-256, you can proceed.

- Change the value of the accepted password authentication to scram-sha-256, as follows.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group --db-parameter-group-name 'docs-lab-scram-passwords'
 \
--parameters
'ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediate'
```

For Windows:

```
aws rds modify-db-parameter-group --db-parameter-group-name "docs-lab-scram-passwords"
 ^
--parameters
"ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediate"
```

Working with the PostgreSQL autovacuum on Amazon RDS for PostgreSQL

We strongly recommend that you use the autovacuum feature to maintain the health of your PostgreSQL DB instance. Autovacuum automates the start of the VACUUM and the ANALYZE commands. It checks for tables with a large number of inserted, updated, or deleted tuples. After this check, it reclaims storage by removing obsolete data or tuples from the PostgreSQL database.

By default, autovacuum is turned on for the Amazon RDS for PostgreSQL DB instances that you create using any of the default PostgreSQL DB parameter groups. These include `default.postgres10`, `default.postgres11`, and so on. All default PostgreSQL DB parameter groups have an `rds.adaptive_autovacuum` parameter that's set to 1, thus activating the feature. Other configuration parameters associated with the autovacuum feature are also set by default. Because these defaults are somewhat generic, you can benefit from tuning some of the parameters associated with the autovacuum feature for your specific workload.

Following, you can find more information about the autovacuum and how to tune some of its parameters on your RDS for PostgreSQL DB instance. For high-level information, see [Best practices for working with PostgreSQL \(p. 224\)](#).

Topics

- [Allocating memory for autovacuum \(p. 1925\)](#)
- [Reducing the likelihood of transaction ID wraparound \(p. 1926\)](#)
- [Determining if the tables in your database need vacuuming \(p. 1926\)](#)
- [Determining which tables are currently eligible for autovacuum \(p. 1927\)](#)
- [Determining if autovacuum is currently running and for how long \(p. 1928\)](#)
- [Performing a manual vacuum freeze \(p. 1929\)](#)
- [Reindexing a table when autovacuum is running \(p. 1930\)](#)
- [Other parameters that affect autovacuum \(p. 1931\)](#)
- [Setting table-level autovacuum parameters \(p. 1932\)](#)
- [Logging autovacuum and vacuum activities \(p. 1932\)](#)

Allocating memory for autovacuum

One of the most important parameters influencing autovacuum performance is the `maintenance_work_mem` parameter. This parameter determines how much memory that you allocate for autovacuum to use to scan a database table and to hold all the row IDs that are going to be vacuumed. If you set the value of the `maintenance_work_mem` parameter too low, the vacuum process might have to scan the table multiple times to complete its work. Such multiple scans can have a negative impact on performance.

When doing calculations to determine the `maintenance_work_mem` parameter value, keep in mind two things:

- The default unit is kilobytes (KB) for this parameter.
- The `maintenance_work_mem` parameter works in conjunction with the `autovacuum_max_workers` parameter. If you have many small tables, allocate more `autovacuum_max_workers` and less `maintenance_work_mem`. If you have large tables (say, larger than 100 GB), allocate more memory and fewer worker processes. You need to have enough memory allocated to succeed on your biggest table. Each `autovacuum_max_workers` can use the memory that you allocate. Thus, make sure that the combination of worker processes and memory equal the total memory that you want to allocate.

In general terms, for large hosts set the `maintenance_work_mem` parameter to a value between one and two gigabytes (between 1,048,576 and 2,097,152 KB). For extremely large hosts, set the parameter to a value between two and four gigabytes (between 2,097,152 and 4,194,304 KB). The value that you set for this parameter depends on the workload. Amazon RDS has updated its default for this parameter to be kilobytes calculated as follows.

`GREATEST({DBInstanceClassMemory/63963136*1024}, 65536).`

Reducing the likelihood of transaction ID wraparound

In some cases, parameter group settings related to autovacuum might not be aggressive enough to prevent transaction ID wraparound. To address this, RDS for PostgreSQL provides a mechanism that adapts the autovacuum parameter values automatically. *Adaptive autovacuum parameter tuning* is a feature for RDS for PostgreSQL. A detailed explanation of [TransactionID wraparound](#) is found in the PostgreSQL documentation.

Adaptive autovacuum parameter tuning is turned on by default for RDS for PostgreSQL instances with the dynamic parameter `rds.adaptive_autovacuum` set to ON. We strongly recommend that you keep this turned on. However, to turn off adaptive autovacuum parameter tuning, set the `rds.adaptive_autovacuum` parameter to 0 or OFF.

Transaction ID wraparound is still possible even when Amazon RDS tunes the autovacuum parameters. We encourage you to implement an Amazon CloudWatch alarm for transaction ID wraparound. For more information, see the post [Implement an early warning system for transaction ID wraparound in RDS for PostgreSQL](#) on the AWS Database Blog.

With adaptive autovacuum parameter tuning turned on, Amazon RDS begins adjusting autovacuum parameters when the CloudWatch metric `MaximumUsedTransactionIDs` reaches the value of the `autovacuum_freeze_max_age` parameter or 500,000,000, whichever is greater.

Amazon RDS continues to adjust parameters for autovacuum if a table continues to trend toward transaction ID wraparound. Each of these adjustments dedicates more resources to autovacuum to avoid wraparound. Amazon RDS updates the following autovacuum-related parameters:

- `autovacuum_vacuum_cost_delay`
- `autovacuum_vacuum_cost_limit`
- `autovacuum_work_mem`
- `autovacuum_naptime`

RDS modifies these parameters only if the new value makes autovacuum more aggressive. The parameters are modified in memory on the DB instance. The values in the parameter group aren't changed. To view the current in-memory settings, use the PostgreSQL `SHOW` SQL command.

When Amazon RDS modifies any of these autovacuum parameters, it generates an event for the affected DB instance. This event is visible on the AWS Management Console and through the Amazon RDS API. After the `MaximumUsedTransactionIDs` CloudWatch metric returns below the threshold, Amazon RDS resets the autovacuum-related parameters in memory back to the values specified in the parameter group. It then generates another event corresponding to this change.

Determining if the tables in your database need vacuuming

You can use the following query to show the number of unvacuumed transactions in a database. The `datfrozenxid` column of a database's `pg_database` row is a lower bound on the normal transaction IDs appearing in that database. This column is the minimum of the per-table `realfrozenxid` values within the database.

```
SELECT datname, age(datfrozenxid) FROM pg_database ORDER BY age(datfrozenxid) desc limit 20;
```

For example, the results of running the preceding query might be the following.

datname	age
mydb	1771757888
template0	1721757888

```
template1 | 1721757888
rdsadmin | 1694008527
postgres | 1693881061
(5 rows)
```

When the age of a database reaches 2 billion transaction IDs, transaction ID (XID) wraparound occurs and the database becomes read-only. You can use this query to produce a metric and run a few times a day. By default, autovacuum is set to keep the age of transactions to no more than 200,000,000 ([autovacuum_freeze_max_age](#)).

A sample monitoring strategy might look like this:

- Set the autovacuum_freeze_max_age value to 200 million transactions.
- If a table reaches 500 million unvacuumed transactions, that triggers a low-severity alarm. This isn't an unreasonable value, but it can indicate that autovacuum isn't keeping up.
- If a table ages to 1 billion, this should be treated as an alarm to take action on. In general, you want to keep ages closer to autovacuum_freeze_max_age for performance reasons. We recommend that you investigate using the recommendations that follow.
- If a table reaches 1.5 billion unvacuumed transactions, that triggers a high-severity alarm. Depending on how quickly your database uses transaction IDs, this alarm can indicate that the system is running out of time to run autovacuum. In this case, we recommend that you resolve this immediately.

If a table is constantly breaching these thresholds, modify your autovacuum parameters further. By default, using VACUUM manually (which has cost-based delays disabled) is more aggressive than using the default autovacuum, but it is also more intrusive to the system as a whole.

We recommend the following:

- Be aware and turn on a monitoring mechanism so that you are aware of the age of your oldest transactions.

For information on creating a process that warns you about transaction ID wraparound, see the AWS Database Blog post [Implement an early warning system for transaction ID wraparound in Amazon RDS for PostgreSQL](#).

- For busier tables, perform a manual vacuum freeze regularly during a maintenance window, in addition to relying on autovacuum. For information on performing a manual vacuum freeze, see [Performing a manual vacuum freeze \(p. 1929\)](#).

Determining which tables are currently eligible for autovacuum

Often, it is one or two tables in need of vacuuming. Tables whose `relfrozenxid` value is greater than the number of transactions in `autovacuum_freeze_max_age` are always targeted by autovacuum. Otherwise, if the number of tuples made obsolete since the last VACUUM exceeds the vacuum threshold, the table is vacuumed.

The [autovacuum threshold](#) is defined as:

```
Vacuum-threshold = vacuum-base-threshold + vacuum-scale-factor * number-of-tuples
```

While you are connected to your database, run the following query to see a list of tables that autovacuum sees as eligible for vacuuming.

```
WITH vbt AS (SELECT setting AS autovacuum_vacuum_threshold FROM
pg_settings WHERE name = 'autovacuum_vacuum_threshold'),
vsf AS (SELECT setting AS autovacuum_vacuum_scale_factor FROM
```

```

pg_settings WHERE name = 'autovacuum_vacuum_scale_factor'),
fma AS (SELECT setting AS autovacuum_freeze_max_age FROM pg_settings WHERE name =
'autovacuum_freeze_max_age'),
sto AS (select opt_oid, split_part(setting, '=', 1) as param,
split_part(setting, '=', 2) as value from (select oid opt_oid, unnest(reloptions) setting
from pg_class) opt)
SELECT ''||ns.nspname||'.'||c.relname||'' as relation,
pg_size.pretty(pg_table_size(c.oid)) as table_size,
age(relfrozenxid) as xid_age,
coalesce(cfma.value::float, autovacuum_freeze_max_age::float) autovacuum_freeze_max_age,
(coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
coalesce(cvsf.value::float, autovacuum_vacuum_scale_factor::float) * c.reltuples)
AS autovacuum_vacuum_tuples, n_dead_tup as dead_tuples FROM
pg_class c join pg_namespace ns on ns.oid = c.relnamespace
join pg_stat_all_tables stat on stat.relid = c.oid join vbt on (1=1) join vsf on (1=1) join
fma on (1=1)
left join sto cvbt on cvbt.param = 'autovacuum_vacuum_threshold' and c.oid = cvbt.opt_oid
left join sto cvsfs on cvsfs.param = 'autovacuum_vacuum_scale_factor' and c.oid =
cvsfs.opt_oid
left join sto cfma on cfma.param = 'autovacuum_freeze_max_age' and c.oid = cfma.opt_oid
WHERE c.relkind = 'r' and ns.nspname <> 'pg_catalog'
AND (age(relfrozenxid) >= coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
OR coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
coalesce(cvsfs.value::float, autovacuum_vacuum_scale_factor::float) *
c.reltuples <= n_dead_tup)
ORDER BY age(relfrozenxid) DESC LIMIT 50;

```

Determining if autovacuum is currently running and for how long

If you need to manually vacuum a table, make sure to determine if autovacuum is currently running. If it is, you might need to adjust parameters to make it run more efficiently, or turn off autovacuum temporarily so that you can manually run VACUUM.

Use the following query to determine if autovacuum is running, how long it has been running, and if it is waiting on another session.

```

SELECT datname, usename, pid, state, wait_event, current_timestamp - xact_start AS
xact_runtime, query
FROM pg_stat_activity
WHERE upper(query) LIKE '%VACUUM%'
ORDER BY xact_start;

```

After running the query, you should see output similar to the following.

datname	usename	pid	state	wait_event	xact_runtime	query
mydb	rdsadmin	16473	active		33 days 16:32:11.600656	autovacuum: VACUUM ANALYZE public.mytable1 (to prevent wraparound)
mydb	rdsadmin	22553	active		14 days 09:15:34.073141	autovacuum: VACUUM ANALYZE public.mytable2 (to prevent wraparound)
mydb	rdsadmin	41909	active		3 days 02:43:54.203349	autovacuum: VACUUM ANALYZE public.mytable3
mydb	rdsadmin	618	active		00:00:00	SELECT datname, usename, pid, state, wait_event, current_timestamp - xact_start AS xact_runtime, query+
						FROM pg_stat_activity

```

like '%VACUUM%'          | WHERE query
+
|                         | ORDER BY
xact_start;               +

```

Several issues can cause a long-running autovacuum session (that is, multiple days long). The most common issue is that your `maintenance_work_mem` parameter value is set too low for the size of the table or rate of updates.

We recommend that you use the following formula to set the `maintenance_work_mem` parameter value.

```
GREATEST({DBInstanceClassMemory/63963136*1024},65536)
```

Short running autovacuum sessions can also indicate problems:

- It can indicate that there aren't enough `autovacuum_max_workers` for your workload. In this case, you need to indicate the number of workers.
- It can indicate that there is an index corruption (autovacuum crashes and restarts on the same relation but makes no progress). In this case, run a manual vacuum `freeze verbose table` to see the exact cause.

Performing a manual vacuum freeze

You might want to perform a manual vacuum on a table that has a vacuum process already running. This is useful if you have identified a table with an age approaching 2 billion transactions (or above any threshold you are monitoring).

The following steps are guidelines, with several variations to the process. For example, during testing, suppose that you find that the `maintenance_work_mem` parameter value is set too small and that you need to take immediate action on a table. However, perhaps you don't want to bounce the instance at the moment. Using the queries in previous sections, you determine which table is the problem and notice a long running autovacuum session. You know that you need to change the `maintenance_work_mem` parameter setting, but you also need to take immediate action and vacuum the table in question. The following procedure shows what to do in this situation.

To manually perform a vacuum freeze

1. Open two sessions to the database containing the table you want to vacuum. For the second session, use "screen" or another utility that maintains the session if your connection is dropped.
2. In session one, get the process ID (PID) of the autovacuum session running on the table.

Run the following query to get the PID of the autovacuum session.

```

SELECT datname, username, pid, current_timestamp - xact_start
AS xact_runtime, query
FROM pg_stat_activity WHERE upper(query) LIKE '%VACUUM%' ORDER BY
xact_start;
```

3. In session two, calculate the amount of memory that you need for this operation. In this example, we determine that we can afford to use up to 2 GB of memory for this operation, so we set `maintenance_work_mem` for the current session to 2 GB.

```
SET maintenance_work_mem='2 GB';
```

SET

4. In session two, issue a `vacuum freeze verbose` command for the table. The verbose setting is useful because, although there is no progress report for this in PostgreSQL currently, you can see activity.

```
\timing on
Timing is on.
vacuum freeze verbose pgbench_branches;
```

```
INFO: vacuuming "public.pgbench_branches"
INFO: index "pgbench_branches_pkey" now contains 50 row versions in 2 pages
DETAIL: 0 index row versions were removed.
0 index pages have been deleted, 0 are currently reusable.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
INFO: index "pgbench_branches_test_index" now contains 50 row versions in 2 pages
DETAIL: 0 index row versions were removed.
0 index pages have been deleted, 0 are currently reusable.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
INFO: "pgbench_branches": found 0 removable, 50 nonremovable row versions
      in 43 out of 43 pages
DETAIL: 0 dead row versions cannot be removed yet.
There were 9347 unused item pointers.
0 pages are entirely empty.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
VACUUM
Time: 2.765 ms
```

5. In session one, if autovacuum was blocking the vacuum session, you see in `pg_stat_activity` that waiting is "T" for your vacuum session. In this case, you need to end the autovacuum process as follows.

```
SELECT pg_terminate_backend('the_pid');
```

At this point, your session begins. It's important to note that autovacuum restarts immediately because this table is probably the highest on its list of work.

6. Initiate your `vacuum freeze verbose` command in session two, and then end the autovacuum process in session one.

Reindexing a table when autovacuum is running

If an index has become corrupt, autovacuum continues to process the table and fails. If you attempt a manual vacuum in this situation, you receive an error message like the following.

```
postgres=> vacuum freeze pgbench_branches;
ERROR: index "pgbench_branches_test_index" contains unexpected
      zero page at block 30521
HINT: Please REINDEX it.
```

When the index is corrupted and autovacuum is attempting to run on the table, you contend with an already running autovacuum session. When you issue a `REINDEX` command, you take out an exclusive lock on the table. Write operations are blocked, and also read operations that use that specific index.

To reindex a table when autovacuum is running on the table

1. Open two sessions to the database containing the table that you want to vacuum. For the second session, use "screen" or another utility that maintains the session if your connection is dropped.

2. In session one, get the PID of the autovacuum session running on the table.

Run the following query to get the PID of the autovacuum session.

```
SELECT datname, username, pid, current_timestamp - xact_start
AS xact_runtime, query
FROM pg_stat_activity WHERE upper(query) like '%VACUUM%' ORDER BY
xact_start;
```

3. In session two, issue the reindex command.

```
\timing on
Timing is on.
reindex index pgbench_branches_test_index;
REINDEX
Time: 9.966 ms
```

4. In session one, if autovacuum was blocking the process, you see in pg_stat_activity that waiting is "T" for your vacuum session. In this case, you end the autovacuum process.

```
SELECT pg_terminate_backend('the_pid');
```

At this point, your session begins. It's important to note that autovacuum restarts immediately because this table is probably the highest on its list of work.

5. Initiate your command in session two, and then end the autovacuum process in session 1.

Other parameters that affect autovacuum

The following query shows the values of some of the parameters that directly affect autovacuum and its behavior. The [autovacuum parameters](#) are described fully in the PostgreSQL documentation.

```
SELECT name, setting, unit, short_desc
FROM pg_settings
WHERE name IN (
'autovacuum_max_workers',
'autovacuum_analyze_scale_factor',
'autovacuum_naptime',
'autovacuum_analyze_threshold',
'autovacuum_analyze_scale_factor',
'autovacuum_vacuum_threshold',
'autovacuum_vacuum_scale_factor',
'autovacuum_vacuum_threshold',
'autovacuum_vacuum_cost_delay',
'autovacuum_vacuum_cost_limit',
'vacuum_cost_limit',
'autovacuum_freeze_max_age',
'maintenance_work_mem',
'vacuum_freeze_min_age');
```

While these all affect autovacuum, some of the most important ones are:

- [maintenance_work_mem](#)
- [autovacuum_freeze_max_age](#)
- [autovacuum_max_workers](#)
- [autovacuum_vacuum_cost_delay](#)
- [autovacuum_vacuum_cost_limit](#)

Setting table-level autovacuum parameters

You can set autovacuum-related [storage parameters](#) at a table level, which can be better than altering the behavior of the entire database. For large tables, you might need to set aggressive settings and you might not want to make autovacuum behave that way for all tables.

The following query shows which tables currently have table-level options in place.

```
SELECT relname, reloptions
FROM pg_class
WHERE reloptions IS NOT null;
```

An example where this might be useful is on tables that are much larger than the rest of your tables. Suppose that you have one 300-GB table and 30 other tables less than 1 GB. In this case, you might set some specific parameters for your large table so you don't alter the behavior of your entire system.

```
ALTER TABLE mytable set (autovacuum_vacuum_cost_delay=0);
```

Doing this turns off the cost-based autovacuum delay for this table at the expense of more resource usage on your system. Normally, autovacuum pauses for autovacuum_vacuum_cost_delay each time autovacuum_cost_limit is reached. For more details, see the PostgreSQL documentation about [cost-based vacuuming](#).

Logging autovacuum and vacuum activities

Information about autovacuum activities is sent to the `postgresql.log` based on the level specified in the `rds.force_autovacuum_logging_level` parameter. Following are the values allowed for this parameter and the PostgreSQL versions for which that value is the default setting:

- disabled (PostgreSQL 10, PostgreSQL 9.6)
- debug5, debug4, debug3, debug2, debug1
- info (PostgreSQL 12, PostgreSQL 11)
- notice
- warning (PostgreSQL 14, PostgreSQL 13)
- error, log, fatal, panic

The `rds.force_autovacuum_logging_level` works with the `log_autovacuum_min_duration` parameter. The `log_autovacuum_min_duration` parameter's value is the threshold (in milliseconds) above which autovacuum actions get logged. A setting of -1 logs nothing, while a setting of 0 logs all actions. As with `rds.force_autovacuum_logging_level`, default values for `log_autovacuum_min_duration` are version dependent, as follows:

- 10000 ms – PostgreSQL 14, PostgreSQL 13, PostgreSQL 12, and PostgreSQL 11
- (empty) – No default value for PostgreSQL 10 and PostgreSQL 9.6

We recommend that you set `rds.force_autovacuum_logging_level` to WARNING. We also recommend that you set `log_autovacuum_min_duration` to a value from 1000 to 5000. A setting of 5000 logs activity that takes longer than 5,000 milliseconds. Any setting other than -1 also logs messages if the autovacuum action is skipped because of a conflicting lock or concurrently dropped relations. For more information, see [Automatic Vacuuming](#) in the PostgreSQL documentation.

To troubleshoot issues, you can change the `rds.force_autovacuum_logging_level` parameter to one of the debug levels, from `debug1` up to `debug5` for the most verbose information. We recommend

that you use debug settings for short periods of time and for troubleshooting purposes only. To learn more, see [When to log](#) in the PostgreSQL documentation.

Note

PostgreSQL allows the `rds_superuser` account to view autovacuum sessions in `pg_stat_activity`. For example, you can identify and end an autovacuum session that is blocking a command from running, or running slower than a manually issued vacuum command.

Working with logging mechanisms supported by RDS for PostgreSQL

There are several parameters, extensions, and other configurable items that you can set to log activities that occur on your PostgreSQL DB instance. These include the following:

- The `log_statement` parameter can be used to log user activity in your PostgreSQL database. To learn more about RDS for PostgreSQL logging and how to monitor the logs, see [RDS for PostgreSQL database log files \(p. 716\)](#).
- The `rds.force_admin_logging_level` parameter logs actions by the Amazon RDS internal user (`rdsadmin`) in the databases on the DB instance. It writes the output to the PostgreSQL error log. Allowed values are `disabled`, `debug5`, `debug4`, `debug3`, `debug2`, `debug1`, `info`, `notice`, `warning`, `error`, `log`, `fatal`, and `panic`. The default value is `disabled`.
- The `rds.force_autovacuum_logging_level` parameter can be set to capture various autovacuum operations in the PostgreSQL error log. For more information, see [Logging autovacuum and vacuum activities \(p. 1932\)](#).
- The PostgreSQL Audit (`pgAudit`) extension can be installed and configured to capture activities at the session level or at the object level. For more information, see [Using pgAudit to log database activity \(p. 1951\)](#).
- The `log_fdw` extension makes it possible for you to access the database engine log using SQL. For more information, see [Using the log_fdw extension to access the DB log using SQL \(p. 1987\)](#).
- The `pg_stat_statements` library is specified as the default for the `shared_preload_libraries` parameter in RDS for PostgreSQL version 10 and higher. It's this library that you can use to analyze running queries. Be sure that `pg_stat_statements` is set in your DB parameter group. For more information about monitoring your RDS for PostgreSQL DB instance using the information that this library provides, see [SQL statistics for RDS PostgreSQL \(p. 632\)](#).
- The `log_hostname` parameter captures to the log the hostname of each client connection. For RDS for PostgreSQL version 12 and higher versions, this parameter is set to `off` by default. If you turn it on, be sure to monitor session connection times. When turned on, the service uses the domain name system (DNS) reverse lookup request to get the hostname of the client that's making the connection and add it to the PostgreSQL log. This has a noticeable impact during session connection. We recommend that you turn on this parameter for troubleshooting purposes only.

In general terms, the point of logging is so that the DBA can monitor, tune performance, and troubleshoot. Many of the logs are uploaded automatically to Amazon CloudWatch or Performance Insights. Here, they're sorted and grouped to provide complete metrics for your DB instance. To learn more about Amazon RDS monitoring and metrics, see [Monitoring metrics in an Amazon RDS instance \(p. 510\)](#).

Using pgBadger for log analysis with PostgreSQL

You can use a log analyzer such as `pgBadger` to analyze PostgreSQL logs. The `pgBadger` documentation states that the `%l` pattern (the log line for the session or process) should be a part of the prefix. However, if you provide the current RDS `log_line_prefix` as a parameter to `pgBadger` it should still produce a report.

For example, the following command correctly formats an Amazon RDS for PostgreSQL log file dated 2014-02-04 using pgBadger.

```
./pgbadger -f stderr -p '%t:%r:%u@%d:[%p]:' postgresql.log.2014-02-04-00
```

Working with parameters on your RDS for PostgreSQL DB instance

In some cases, you might create an RDS for PostgreSQL DB instance without specifying a custom parameter group. If so, your DB instance is created using the default parameter group for the version of PostgreSQL that you choose. For example, suppose that you create an RDS for PostgreSQL DB instance using PostgreSQL 13.3. In this case, the DB instance is created using the values in the parameter group for PostgreSQL 13 releases, `default.postgres13`.

You can also create your own custom DB parameter group. You need to do this if you want to modify any settings for the RDS for PostgreSQL DB instance from their default values. To learn how, see [Working with parameter groups \(p. 289\)](#).

You can track the settings on your RDS for PostgreSQL DB instance in several different ways. You can use the AWS Management Console, the AWS CLI, or the Amazon RDS API. You can also query the values from the PostgreSQL `pg_settings` table of your instance, as shown following.

```
SELECT name, setting, boot_val, reset_val, unit
  FROM pg_settings
 ORDER BY name;
```

To learn more about the values returned from this query, see [pg_settings](#) in the PostgreSQL documentation.

Be especially careful when changing the settings for `max_connections` and `shared_buffers` on your RDS for PostgreSQL DB instance. For example, suppose that you modify settings for `max_connections` or `shared_buffers` and you use values that are too high for your actual workload. In this case, your RDS for PostgreSQL DB instance won't start. If this happens, you see an error such as the following in the `postgres.log`.

```
2018-09-18 21:13:15 UTC::@:[8097]:FATAL:  could not map anonymous shared memory: Cannot
allocate memory
2018-09-18 21:13:15 UTC::@:[8097]:HINT:  This error usually means that PostgreSQL's request
for a shared memory segment
exceeded available memory or swap space. To reduce the request size (currently
3514134274048 bytes), reduce
PostgreSQL's shared memory usage, perhaps by reducing shared_buffers or max_connections.
```

However, you can't change any values of the settings contained in the default RDS for PostgreSQL DB parameter groups. To change settings for any parameters, first create a custom DB parameter group. Then change the settings in that custom group, and then apply the custom parameter group to your RDS for PostgreSQL DB instance. To learn more, see [Working with parameter groups \(p. 289\)](#).

There are two types of RDS for PostgreSQL DB parameters.

- **Static parameters** – Static parameters require that the RDS for PostgreSQL DB instance be rebooted after a change so that the new value can take effect.
- **Dynamic parameters** – Dynamic parameters don't require a reboot after changing their settings.

Note

If your RDS for PostgreSQL DB instance is using your own custom DB parameter group, you can change the values of dynamic parameters on the running DB instance. You can do this by using the AWS Management Console, the AWS CLI, or the Amazon RDS API.

If you have privileges to do so, you can also change parameter values by using the `ALTER DATABASE`, `ALTER ROLE`, and `SET` commands.

RDS for PostgreSQL DB instance parameter list

The following table lists some (but not all) parameters available in an RDS for PostgreSQL DB instance. To view all available parameters, you use the [describe-db-parameters](#) AWS CLI command. For example, to get the list of all parameters available in the default parameter group for RDS for PostgreSQL version 13, run the following.

```
aws rds describe-db-parameters --db-parameter-group-name default.postgres13
```

You can also use the Console. Choose **Parameter groups** from the Amazon RDS menu, and then choose the parameter group from those available in your AWS Region.

Parameter name	Apply_Type	Description
application_name	Dynamic	Sets the application name to be reported in statistics and logs.
archive_command	Dynamic	Sets the shell command that will be called to archive a WAL file.
array_nulls	Dynamic	Enables input of NULL elements in arrays.
authentication_timeout	Dynamic	Sets the maximum allowed time to complete client authentication.
autovacuum	Dynamic	Starts the autovacuum subprocess.
autovacuum_analyze_scale_factor	Dynamic	Number of tuple inserts, updates, or deletes before analyze as a fraction of reltuples.
autovacuum_analyze_threshold	Dynamic	Minimum number of tuple inserts, updates, or deletes before analyze.
autovacuum_freeze_max_age	Static	Age at which to autovacuum a table to prevent transaction ID wraparound.
autovacuum_naptime	Dynamic	Time to sleep between autovacuum runs.
autovacuum_max_workers	Static	Sets the maximum number of simultaneously running autovacuum worker processes.
autovacuum_vacuum_cost_delay	Dynamic	Vacuum cost delay, in milliseconds, for autovacuum.
autovacuum_vacuum_cost_limit	Dynamic	Vacuum cost amount available before napping, for autovacuum.
autovacuum_vacuum_scale_factor	Dynamic	Number of tuple updates or deletes before vacuum as a fraction of reltuples.
autovacuum_vacuum_threshold	Dynamic	Minimum number of tuple updates or deletes before vacuum.
backslash_quote	Dynamic	Sets whether a backslash (\) is allowed in string literals.
bgwriter_delay	Dynamic	Background writer sleep time between rounds.
bgwriter_lru_maxpages	Dynamic	Background writer maximum number of LRU pages to flush per round.

Parameter name	Apply_Type	Description
bgwriter_lru_multiplier	Dynamic	Multiple of the average buffer usage to free per round.
bytea_output	Dynamic	Sets the output format for bytes.
check_function_bodies	Dynamic	Checks function bodies during CREATE FUNCTION.
checkpoint_completion_target	Dynamic	Time spent flushing dirty buffers during checkpoint, as a fraction of the checkpoint interval.
checkpoint_segments	Dynamic	Sets the maximum distance in log segments between automatic write-ahead log (WAL) checkpoints.
checkpoint_timeout	Dynamic	Sets the maximum time between automatic WAL checkpoints.
checkpoint_warning	Dynamic	Enables warnings if checkpoint segments are filled more frequently than this.
client_encoding	Dynamic	Sets the client's character set encoding.
client_min_messages	Dynamic	Sets the message levels that are sent to the client.
commit_delay	Dynamic	Sets the delay in microseconds between transaction commit and flushing WAL to disk.
commit_siblings	Dynamic	Sets the minimum concurrent open transactions before performing commit_delay.
constraint_exclusion	Dynamic	Enables the planner to use constraints to optimize queries.
cpu_index_tuple_cost	Dynamic	Sets the planner's estimate of the cost of processing each index entry during an index scan.
cpu_operator_cost	Dynamic	Sets the planner's estimate of the cost of processing each operator or function call.
cpu_tuple_cost	Dynamic	Sets the planner's estimate of the cost of processing each tuple (row).
cursor_tuple_fraction	Dynamic	Sets the planner's estimate of the fraction of a cursor's rows that will be retrieved.
datestyle	Dynamic	Sets the display format for date and time values.
deadlock_timeout	Dynamic	Sets the time to wait on a lock before checking for deadlock.
debug_pretty_print	Dynamic	Indents parse and plan tree displays.
debug_print_parse	Dynamic	Logs each query's parse tree.
debug_print_plan	Dynamic	Logs each query's execution plan.
debug_print_rewritten	Dynamic	Logs each query's rewritten parse tree.
default_statistics_target	Dynamic	Sets the default statistics target.
default_tablespace	Dynamic	Sets the default tablespace to create tables and indexes in.
default_transaction_deferrable	Dynamic	Sets the default deferrable status of new transactions.

Parameter name	Apply_Type	Description
default_transaction_isolation	Dynamic	Sets the transaction isolation level of each new transaction.
default_transaction_read_only	Dynamic	Sets the default read-only status of new transactions.
default_with_oids	Dynamic	Creates new tables with object IDs (OIDs) by default.
effective_cache_size	Dynamic	Sets the planner's assumption about the size of the disk cache.
effective_ioConcurrency	Dynamic	Number of simultaneous requests that can be handled efficiently by the disk subsystem.
enable_bitmapscan	Dynamic	Enables the planner's use of bitmap-scan plans.
enable_hashagg	Dynamic	Enables the planner's use of hashed aggregation plans.
enable_hashjoin	Dynamic	Enables the planner's use of hash join plans.
enable_indexscan	Dynamic	Enables the planner's use of index-scan plans.
enable_material	Dynamic	Enables the planner's use of materialization.
enable_mergejoin	Dynamic	Enables the planner's use of merge join plans.
enable_nestloop	Dynamic	Enables the planner's use of nested-loop join plans.
enable_seqscan	Dynamic	Enables the planner's use of sequential-scan plans.
enable_sort	Dynamic	Enables the planner's use of explicit sort steps.
enable_tidscan	Dynamic	Enables the planner's use of TID scan plans.
escape_string_warning	Dynamic	Warns about backslash (\) escapes in ordinary string literals.
extra_float_digits	Dynamic	Sets the number of digits displayed for floating-point values.
fromCollapse_limit	Dynamic	Sets the FROM-list size beyond which subqueries are not collapsed.
fsync	Dynamic	Forces synchronization of updates to disk.
full_page_writes	Dynamic	Writes full pages to WAL when first modified after a checkpoint.
geqo	Dynamic	Enables genetic query optimization.
geqo_effort	Dynamic	GEQO: effort is used to set the default for other GEQO parameters.
geqo_generations	Dynamic	GEQO: number of iterations of the algorithm.
geqo_pool_size	Dynamic	GEQO: number of individuals in the population.
geqo_seed	Dynamic	GEQO: seed for random path selection.
geqo_selection_bias	Dynamic	GEQO: selective pressure within the population.
geqo_threshold	Dynamic	Sets the threshold of FROM items beyond which GEQO is used.

Parameter name	Apply_Type	Description
gin_fuzzy_search_limit	Dynamic	Sets the maximum allowed result for exact search by GIN.
hot_standby_feedback	Dynamic	Determines whether a hot standby sends feedback messages to the primary or upstream standby.
intervalstyle	Dynamic	Sets the display format for interval values.
joinCollapse_limit	Dynamic	Sets the FROM-list size beyond which JOIN constructs are not flattened.
lc_messages	Dynamic	Sets the language in which messages are displayed.
lc_monetary	Dynamic	Sets the locale for formatting monetary amounts.
lc_numeric	Dynamic	Sets the locale for formatting numbers.
lc_time	Dynamic	Sets the locale for formatting date and time values.
log_autovacuum_min_duration	Dynamic	Sets the minimum running time above which autovacuum actions will be logged.
log_checkpoints	Dynamic	Logs each checkpoint.
log_connections	Dynamic	Logs each successful connection.
log_disconnections	Dynamic	Logs end of a session, including duration.
log_duration	Dynamic	Logs the duration of each completed SQL statement.
log_error_verbosity	Dynamic	Sets the verbosity of logged messages.
log_executor_stats	Dynamic	Writes executor performance statistics to the server log.
log_filename	Dynamic	Sets the file name pattern for log files.
log_file_mode	Dynamic	Sets file permissions for log files. Default value is 0644.
log_hostname	Dynamic	Logs the host name in the connection logs. As of PostgreSQL 12 and later versions, this parameter is 'off' by default. When turned on, the connection uses DNS reverse-lookup to get the hostname that gets captured to the connection logs. If you turn on this parameter, you should monitor the impact that it has on the time it takes to establish connections.
log_line_prefix	Dynamic	Controls information prefixed to each log line.
log_lock_waits	Dynamic	Logs long lock waits.
log_min_duration_statement	Dynamic	Sets the minimum running time above which statements will be logged.
log_min_error_statement	Dynamic	Causes all statements generating an error at or above this level to be logged.
log_min_messages	Dynamic	Sets the message levels that are logged.
log_parser_stats	Dynamic	Writes parser performance statistics to the server log.
log_planner_stats	Dynamic	Writes planner performance statistics to the server log.

Parameter name	Apply_Type	Description
log_rotation_age	Dynamic	Automatic log file rotation will occur after N minutes.
log_rotation_size	Dynamic	Automatic log file rotation will occur after N kilobytes.
log_statement	Dynamic	Sets the type of statements logged.
log_statement_stats	Dynamic	Writes cumulative performance statistics to the server log.
log_temp_files	Dynamic	Logs the use of temporary files larger than this number of kilobytes.
log_timezone	Dynamic	Sets the time zone to use in log messages.
log_truncate_on_rotation	Dynamic	Truncate existing log files of same name during log rotation.
logging_collector	Static	Start a subprocess to capture stderr output and/or csvlogs into log files.
maintenance_work_mem	Dynamic	Sets the maximum memory to be used for maintenance operations.
max_connections	Static	Sets the maximum number of concurrent connections.
max_files_per_process	Static	Sets the maximum number of simultaneously open files for each server process.
max_locks_per_transaction	Static	Sets the maximum number of locks per transaction.
max_pred_locks_per_transaction	Static	Sets the maximum number of predicate locks per transaction.
max_prepared_transactions	Static	Sets the maximum number of simultaneously prepared transactions.
max_stack_depth	Dynamic	Sets the maximum stack depth, in kilobytes.
max_standby_archive_delay	Dynamic	Sets the maximum delay before canceling queries when a hot standby server is processing archived WAL data.
max_standby_streaming_delay	Dynamic	Sets the maximum delay before canceling queries when a hot standby server is processing streamed WAL data.
max_wal_size	Dynamic	Sets the WAL size that triggers the checkpoint. For PostgreSQL version 9.6 and earlier, max_wal_size is in units of 16 MB. For PostgreSQL version 10 and later, max_wal_size is in units of 1 MB.
min_wal_size	Dynamic	Sets the minimum size to shrink the WAL to. For PostgreSQL version 9.6 and earlier, min_wal_size is in units of 16 MB. For PostgreSQL version 10 and later, min_wal_size is in units of 1 MB.
quote_all_identifiers	Dynamic	Adds quotes ("") to all identifiers when generating SQL fragments.

Parameter name	Apply_Type	Description
random_page_cost	Dynamic	Sets the planner's estimate of the cost of a non-sequentially fetched disk page. This parameter has no value unless query plan management (QPM) is turned on. When QPM is on, the default value for this parameter is 4.
rds.adaptive_autovacuum	Dynamic	Automatically tunes the autovacuum parameters whenever the transaction ID thresholds are exceeded.
rds.force_ssl	Dynamic	Requires the use of SSL connections. Default is 0 (false), so connections aren't required (forced) to use SSL.
rds.log_retention_period	Dynamic	Sets log retention such that Amazon RDS deletes PostgreSQL logs that are older than <i>n</i> minutes.
rds.restrict_password_command	Static	Restricts who can manage passwords to users with the rds_password role. Set this parameter to 1 to enable password restriction. The default is 0.
search_path	Dynamic	Sets the schema search order for names that are not schema-qualified.
seq_page_cost	Dynamic	Sets the planner's estimate of the cost of a sequentially fetched disk page.
session_replication_role	Dynamic	Sets the sessions behavior for triggers and rewrite rules.
shared_buffers	Static	Sets the number of shared memory buffers used by the server.
shared_preload_libraries	Static	Lists the shared libraries to preload into the RDS for PostgreSQL DB instance. Supported values include auto_explain, orafce, pgaudit, pglogical, pg_bigm, pg_cron, pg_hint_plan, pg_prewarm, pg_similarity, pg_stat_statements, pg_transport, and plprofiler.
ssl	Dynamic	Enables SSL connections.
sql_inheritance	Dynamic	Causes subtables to be included by default in various commands.
ssl_renegotiation_limit	Dynamic	Sets the amount of traffic to send and receive before renegotiating the encryption keys.
standard_conforming_strings	Dynamic	Causes ... strings to treat backslashes literally.
statement_timeout	Dynamic	Sets the maximum allowed duration of any statement.
synchronize_seqscans	Dynamic	Enables synchronized sequential scans.
synchronous_commit	Dynamic	Sets the current transactions synchronization level.
tcp_keepalives_count	Dynamic	Maximum number of TCP keepalive retransmits.
tcp_keepalives_idle	Dynamic	Time between issuing TCP keepalives.
tcp_keepalives_interval	Dynamic	Time between TCP keepalive retransmits.
temp_buffers	Dynamic	Sets the maximum number of temporary buffers used by each session.

Parameter name	Apply_Type	Description
temp_file_limit	Dynamic	Sets the maximum size in KB to which the temporary files can grow.
temp_tablespaces	Dynamic	Sets the tablespaces to use for temporary tables and sort files.
timezone	Dynamic	Sets the time zone for displaying and interpreting time stamps.
track_activities	Dynamic	Collects information about running commands.
track_activity_query_size	Static	Sets the size reserved for pg_stat_activity.current_query, in bytes.
track_counts	Dynamic	Collects statistics on database activity.
track_functions	Dynamic	Collects function-level statistics on database activity.
track_io_timing	Dynamic	Collects timing statistics on database I/O activity.
transaction_deferrable	Dynamic	Indicates whether to defer a read-only serializable transaction until it can be started with no possible serialization failures.
transaction_isolation	Dynamic	Sets the current transactions isolation level.
transaction_read_only	Dynamic	Sets the current transactions read-only status.
transform_null_equals	Dynamic	Treats expr=NULL as expr IS NULL.
update_process_title	Dynamic	Updates the process title to show the active SQL command.
vacuum_cost_delay	Dynamic	Vacuum cost delay in milliseconds.
vacuum_cost_limit	Dynamic	Vacuum cost amount available before napping.
vacuum_cost_page_dirty	Dynamic	Vacuum cost for a page dirtied by vacuum.
vacuum_cost_page_hit	Dynamic	Vacuum cost for a page found in the buffer cache.
vacuum_cost_page_miss	Dynamic	Vacuum cost for a page not found in the buffer cache.
vacuum_defer_cleanup_age	Dynamic	Number of transactions by which vacuum and hot cleanup should be deferred, if any.
vacuum_freeze_min_age	Dynamic	Minimum age at which vacuum should freeze a table row.
vacuum_freeze_table_age	Dynamic	Age at which vacuum should scan a whole table to freeze tuples.
wal_buffers	Static	Sets the number of disk-page buffers in shared memory for WAL.
wal_writer_delay	Dynamic	WAL writer sleep time between WAL flushes.
work_mem	Dynamic	Sets the maximum memory to be used for query workspaces.
xmlbinary	Dynamic	Sets how binary values are to be encoded in XML.

Parameter name	Apply_Type	Description
xmloption	Dynamic	Sets whether XML data in implicit parsing and serialization operations is to be considered as documents or content fragments.

Amazon RDS uses the default PostgreSQL units for all parameters. The following table shows the PostgreSQL default unit and value for each parameter.

Parameter name	Unit
archive_timeout	s
authentication_timeout	s
autovacuum_naptime	s
autovacuum_vacuum_cost_delay	ms
bgwriter_delay	ms
checkpoint_timeout	s
checkpoint_warning	s
deadlock_timeout	ms
effective_cache_size	8 KB
lock_timeout	ms
log_autovacuum_min_duration	ms
log_min_duration_statement	ms
log_rotation_age	minutes
log_rotation_size	KB
log_temp_files	KB
maintenance_work_mem	KB
max_stack_depth	KB
max_standby_archive_delay	ms
max_standby_streaming_delay	ms
post_auth_delay	s
pre_auth_delay	s
segment_size	8 KB
shared_buffers	8 KB
statement_timeout	ms
ssl_renegotiation_limit	KB

Parameter name	Unit
tcp_keepalives_idle	s
tcp_keepalives_interval	s
temp_file_limit	KB
work_mem	KB
temp_buffers	8 KB
vacuum_cost_delay	ms
wal_buffers	8 KB
wal_receiver_timeout	ms
wal_segment_size	8 KB
wal_sender_timeout	ms
wal_writer_delay	ms
wal_receiver_status_interval	s

Using PostgreSQL extensions with Amazon RDS for PostgreSQL

You can extend the functionality of PostgreSQL by installing a variety of extensions and modules. For example, to work with spatial data you can install and use the PostGIS extension. For more information, see [Managing spatial data with the PostGIS extension \(p. 1980\)](#). As another example, if you want to improve data entry for very large tables, you can consider partitioning your data by using the pg_partman extension. To learn more, see [Managing PostgreSQL partitions with the pg_partman extension \(p. 1947\)](#).

In some cases, rather than installing an extension, you might add a specific module to the list of `shared_preload_libraries` in your Aurora PostgreSQL DB cluster's custom DB cluster parameter group. Typically, the default DB cluster parameter group loads only the `pg_stat_statements`, but several other modules are available to add to the list. For example, you can add scheduling capability by adding the `pg_cron` module, as detailed in [Scheduling maintenance with the PostgreSQL pg_cron extension \(p. 1960\)](#). As another example, you can log query execution plans by loading the `auto_explain` module. To learn more, see [Logging execution plans of queries](#) in the AWS knowledge center.

Depending on your version of RDS for PostgreSQL, installing an extension might require `rds_superuser` permissions, as follows:

- For RDS for PostgreSQL versions 12 and earlier versions, installing extensions requires `rds_superuser` privileges.
- For RDS for PostgreSQL version 13 and higher versions, users (roles) with create permissions on a given database instance can install and use any *trusted extensions*. For a list of trusted extensions, see [PostgreSQL trusted extensions \(p. 1808\)](#).

You can also specify precisely which extensions can be installed on your RDS for PostgreSQL DB instance, by listing them in the `rds.allowed_extensions` parameter. By default, this parameter isn't set, so any supported extension can be added if the user has permissions to do so. By adding a list of extensions to this parameter, you explicitly identify the extensions that your RDS for PostgreSQL DB instance can use. Any extensions not listed can't be installed. This capability is available for the following versions:

- RDS for PostgreSQL 14.1 and all higher versions
- RDS for PostgreSQL 13.3 and higher minor versions
- RDS for PostgreSQL 12.7 and higher minor versions

For more information, see [Restricting installation of PostgreSQL extensions \(p. 1807\)](#).

To learn more about the `rds_superuser` role, see [Understanding PostgreSQL roles and permissions \(p. 1915\)](#).

Topics

- [Using functions from the orafce extension \(p. 1946\)](#)
- [Managing PostgreSQL partitions with the pg_partman extension \(p. 1947\)](#)
- [Using pgAudit to log database activity \(p. 1951\)](#)
- [Scheduling maintenance with the PostgreSQL pg_cron extension \(p. 1960\)](#)
- [Using pglogical to synchronize data across instances \(p. 1967\)](#)
- [Reducing bloat in tables and indexes with the pg_repack extension \(p. 1977\)](#)
- [Upgrading and using the PLV8 extension \(p. 1978\)](#)
- [Managing spatial data with the PostGIS extension \(p. 1980\)](#)

Using functions from the orafce extension

The orafce extension provides functions and operators that emulate a subset of functions and packages from an Oracle database. The orafce extension makes it easier for you to port an Oracle application to PostgreSQL. RDS for PostgreSQL versions 9.6.6 and higher support this extension. For more information about orafce, see [orafce](#) on GitHub.

Note

RDS for PostgreSQL doesn't support the `utl_file` package that is part of the orafce extension. This is because the `utl_file` schema functions provide read and write operations on operating-system text files, which requires superuser access to the underlying host. As a managed service, RDS for PostgreSQL doesn't provide host access.

To use the orafce extension

1. Connect to the DB instance with the master user name that you used to create the DB instance.

If you want to turn on orafce for a different database in the same DB instance, use the `/c dbname psql` command. Using this command, you change from the primary database after initiating the connection.

2. Turn on the orafce extension with the `CREATE EXTENSION` statement.

```
CREATE EXTENSION orafce;
```

3. Transfer ownership of the oracle schema to the `rds_superuser` role with the `ALTER SCHEMA` statement.

```
ALTER SCHEMA oracle OWNER TO rds_superuser;
```

If you want to see the list of owners for the oracle schema, use the `\dn psql` command.

Managing PostgreSQL partitions with the pg_partman extension

PostgreSQL table partitioning provides a framework for high-performance handling of data input and reporting. Use partitioning for databases that require very fast input of large amounts of data. Partitioning also provides for faster queries of large tables. Partitioning helps maintain data without impacting the database instance because it requires less I/O resources.

By using partitioning, you can split data into custom-sized chunks for processing. For example, you can partition time-series data for ranges such as hourly, daily, weekly, monthly, quarterly, yearly, custom, or any combination of these. For a time-series data example, if you partition the table by hour, each partition contains one hour of data. If you partition the time-series table by day, the partitions holds one day's worth of data, and so on. The partition key controls the size of a partition.

When you use an INSERT or UPDATE SQL command on a partitioned table, the database engine routes the data to the appropriate partition. PostgreSQL table partitions that store the data are child tables of the main table.

During database query reads, the PostgreSQL optimizer examines the WHERE clause of the query and, if possible, directs the database scan to only the relevant partitions.

Starting with version 10, PostgreSQL uses declarative partitioning to implement table partitioning. This is also known as native PostgreSQL partitioning. Before PostgreSQL version 10, you used triggers to implement partitions.

PostgreSQL table partitioning provides the following features:

- Creation of new partitions at any time.
- Variable partition ranges.
- Detachable and reattachable partitions using data definition language (DDL) statements.

For example, detachable partitions are useful for removing historical data from the main partition but keeping historical data for analysis.

- New partitions inherit the parent database table properties, including the following:
 - Indexes
 - Primary keys, which must include the partition key column
 - Foreign keys
 - Check constraints
 - References
- Creating indexes for the full table or each specific partition.

You can't alter the schema for an individual partition. However, you can alter the parent table (such as adding a new column), which propagates to partitions.

Topics

- [Overview of the PostgreSQL pg_partman extension \(p. 1948\)](#)
- [Enabling the pg_partman extension \(p. 1948\)](#)
- [Configuring partitions using the create_parent function \(p. 1949\)](#)
- [Configuring partition maintenance using the run_maintenance_proc function \(p. 1950\)](#)

Overview of the PostgreSQL pg_partman extension

You can use the PostgreSQL pg_partman extension to automate the creation and maintenance of table partitions. For more general information, see [PG Partition Manager](#) in the pg_partman documentation.

Note

The pg_partman extension is supported on RDS for PostgreSQL versions 12.5 and higher.

Instead of having to manually create each partition, you configure pg_partman with the following settings:

- Table to be partitioned
- Partition type
- Partition key
- Partition granularity
- Partition precreation and management options

After you create a PostgreSQL partitioned table, you register it with pg_partman by calling the `create_parent` function. Doing this creates the necessary partitions based on the parameters you pass to the function.

The pg_partman extension also provides the `run_maintenance_proc` function, which you can call on a scheduled basis to automatically manage partitions. To ensure that the proper partitions are created as needed, schedule this function to run periodically (such as hourly). You can also ensure that partitions are automatically dropped.

Enabling the pg_partman extension

If you have multiple databases inside the same PostgreSQL DB instance for which you want to manage partitions, enable the pg_partman extension separately for each database. To enable the pg_partman extension for a specific database, create the partition maintenance schema and then create the pg_partman extension as follows.

```
CREATE SCHEMA partman;
CREATE EXTENSION pg_partman WITH SCHEMA partman;
```

Note

To create the pg_partman extension, make sure that you have `rds_superuser` privileges.

If you receive an error such as the following, grant the `rds_superuser` privileges to the account or use your superuser account.

```
ERROR: permission denied to create extension "pg_partman"
HINT: Must be superuser to create this extension.
```

To grant `rds_superuser` privileges, connect with your superuser account and run the following command.

```
GRANT rds_superuser TO user-or-role;
```

For the examples that show using the pg_partman extension, we use the following sample database table and partition. This database uses a partitioned table based on a timestamp. A schema `data_mart` contains a table named `events` with a column named `created_at`. The following settings are included in the `events` table:

- Primary keys `event_id` and `created_at`, which must have the column used to guide the partition.
- A check constraint `ck_valid_operation` to enforce values for an operation table column.
- Two foreign keys, where one (`fk_orga_membership`) points to the external table `organization` and the other (`fk_parent_event_id`) is a self-referenced foreign key.
- Two indexes, where one (`idx_org_id`) is for the foreign key and the other (`idx_event_type`) is for the event type.

The follow DDL statements create these objects, which are automatically included on each partition.

```

CREATE SCHEMA data_mart;
CREATE TABLE data_mart.organization (
    org_id BIGSERIAL,
    org_name TEXT,
    CONSTRAINT pk_organization PRIMARY KEY (org_id)
);

CREATE TABLE data_mart.events(
    event_id      BIGSERIAL,
    operation     CHAR(1),
    value         FLOAT(24),
    parent_event_id BIGINT,
    event_type    VARCHAR(25),
    org_id        BIGSERIAL,
    created_at    timestamp,
    CONSTRAINT pk_data_mart_event PRIMARY KEY (event_id, created_at),
    CONSTRAINT ck_valid_operation CHECK (operation = 'C' OR operation = 'D'),
    CONSTRAINT fk_orga_membership
        FOREIGN KEY(org_id)
        REFERENCES data_mart.organization (org_id),
    CONSTRAINT fk_parent_event_id
        FOREIGN KEY(parent_event_id, created_at)
        REFERENCES data_mart.events (event_id, created_at)
) PARTITION BY RANGE (created_at);

CREATE INDEX idx_org_id      ON data_mart.events(org_id);
CREATE INDEX idx_event_type ON data_mart.events(event_type);

```

Configuring partitions using the `create_parent` function

After you enable the `pg_partman` extension, use the `create_parent` function to configure partitions inside the partition maintenance schema. The following example uses the `events` table example created in [Enabling the pg_partman extension \(p. 1948\)](#). Call the `create_parent` function as follows.

```

SELECT partman.create_parent(
    p_parent_table => 'data_mart.events',
    p_control => 'created_at',
    p_type => 'native',
    p_interval=> 'daily',
    p_premake => 30);

```

The parameters are as follows:

- `p_parent_table` – The parent partitioned table. This table must already exist and be fully qualified, including the schema.
- `p_control` – The column on which the partitioning is to be based. The data type must be an integer or time-based.
- `p_type` – The type is either '`native`' or '`partman`'. You typically use the `native` type for its performance improvements and flexibility. The `partman` type relies on inheritance.

- `p_interval` – The time interval or integer range for each partition. Example values include daily, hourly, and so on.
- `p_premake` – The number of partitions to create in advance to support new inserts.

For a complete description of the `create_parent` function, see [Creation Functions](#) in the pg_partman documentation.

Configuring partition maintenance using the `run_maintenance_proc` function

You can run partition maintenance operations to automatically create new partitions, detach partitions, or remove old partitions. Partition maintenance relies on the `run_maintenance_proc` function of the pg_partman extension and the pg_cron extension, which initiates an internal scheduler. The pg_cron scheduler automatically executes SQL statements, functions, and procedures defined in your databases.

The following example uses the events table example created in [Enabling the pg_partman extension \(p. 1948\)](#) to set partition maintenance operations to run automatically. As a prerequisite, add `pg_cron` to the `shared_preload_libraries` parameter in the DB instance's parameter group.

```
CREATE EXTENSION pg_cron;

UPDATE partman.part_config
SET infinite_time_partitions = true,
    retention = '3 months',
    retention_keep_table=true
WHERE parent_table = 'data_mart.events';
SELECT cron.schedule('@hourly', $$CALL partman.run_maintenance_proc()$$);
```

Following, you can find a step-by-step explanation of the preceding example:

1. Modify the parameter group associated with your DB instance and add `pg_cron` to the `shared_preload_libraries` parameter value. This change requires a DB instance restart for it to take effect. For more information, see [Modifying parameters in a DB parameter group \(p. 294\)](#).
2. Run the command `CREATE EXTENSION pg_cron;` using an account that has the `rds_superuser` permissions. Doing this enables the `pg_cron` extension. For more information, see [Scheduling maintenance with the PostgreSQL pg_cron extension \(p. 1960\)](#).
3. Run the command `UPDATE partman.part_config` to adjust the pg_partman settings for the `data_mart.events` table.
4. Run the command `SET ...` to configure the `data_mart.events` table, with these clauses:
 - a. `infinite_time_partitions = true`, – Configures the table to be able to automatically create new partitions without any limit.
 - b. `retention = '3 months'`, – Configures the table to have a maximum retention of three months.
 - c. `retention_keep_table=true` – Configures the table so that when the retention period is due, the table isn't deleted automatically. Instead, partitions that are older than the retention period are only detached from the parent table.
5. Run the command `SELECT cron.schedule ...` to make a `pg_cron` function call. This call defines how often the scheduler runs the pg_partman maintenance procedure, `partman.run_maintenance_proc`. For this example, the procedure runs every hour.

For a complete description of the `run_maintenance_proc` function, see [Maintenance Functions](#) in the pg_partman documentation.

Using pgAudit to log database activity

Financial institutions, government agencies, and many industries need to keep *audit logs* to meet regulatory requirements. By using the PostgreSQL Audit extension (pgAudit) with your RDS for PostgreSQL DB instance, you can capture the detailed records that are typically needed by auditors or to meet regulatory requirements. For example, you can set up the pgAudit extension to track changes made to specific databases and tables, to record the user who made the change, and many other details.

The pgAudit extension builds on the functionality of the native PostgreSQL logging infrastructure by extending the log messages with more detail. In other words, you use the same approach to view your audit log as you do to view any log messages. For more information about PostgreSQL logging, see [RDS for PostgreSQL database log files \(p. 716\)](#).

The pgAudit extension redacts sensitive data such as cleartext passwords from the logs. If your RDS for PostgreSQL DB instance is configured to log data manipulation language (DML) statements as detailed in [Turning on query logging for your RDS for PostgreSQL DB instance \(p. 718\)](#), you can avoid the cleartext password issue by using the PostgreSQL Audit extension.

You can configure auditing on your database instances with a great degree of specificity. You can audit all databases and all users. Or, you can choose to audit only certain databases, users, and other objects. You can also explicitly exclude certain users and databases from being audited. For more information, see [Excluding users or databases from audit logging \(p. 1956\)](#).

Given the amount of detail that can be captured, we recommend that if you do use pgAudit, you monitor your storage consumption.

The pgAudit extension is supported on all available RDS for PostgreSQL versions. For a list of pgAudit versions supported by available RDS for PostgreSQL versions, see [Extension versions for Amazon RDS for PostgreSQL in the Amazon RDS for PostgreSQL Release Notes](#).

Topics

- [Setting up the pgAudit extension \(p. 1951\)](#)
- [Auditing database objects \(p. 1954\)](#)
- [Excluding users or databases from audit logging \(p. 1956\)](#)
- [Reference for the pgAudit extension \(p. 1958\)](#)

Setting up the pgAudit extension

To set up the pgAudit extension on your RDS for PostgreSQL DB instance , you first add pgAudit to the shared libraries on the custom DB parameter group for your RDS for PostgreSQL DB instance. For information about creating a custom DB parameter group, see [Working with parameter groups \(p. 289\)](#). Next, you install the pgAudit extension. Finally, you specify the databases and objects that you want to audit. The procedures in this section show you how. You can use the AWS Management Console or the AWS CLI.

You must have permissions as the `rds_superuser` role to perform all these tasks.

The steps following assume that your RDS for PostgreSQL DB instance is associated with a custom DB parameter group.

Console

To set up the pgAudit extension

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

2. In the navigation pane, choose your RDS for PostgreSQL DB instance.
3. Open the **Configuration** tab for your RDS for PostgreSQL DB instance. Among the Instance details, find the **Parameter group** link.
4. Choose the link to open the custom parameters associated with your RDS for PostgreSQL DB instance.
5. In the **Parameters** search field, type `shared_pre` to find the `shared_preload_libraries` parameter.
6. Choose **Edit parameters** to access the property values.
7. Add `pgaudit` to the list in the **Values** field. Use a comma to separate items in the list of values.

The screenshot shows the AWS RDS Parameter Groups interface. A search bar at the top contains the text "shared_pre". Below it, a table lists a single parameter: "shared_preload_libraries" with the value "pgaudit,pg_stat_statements". To the right of the value, a list of allowed values is shown, with "pgaudit" and "pg_stat_statements" highlighted by a red box. Other allowed values include auto_explain, orafce, pgaudit, pglogical, pg_bigm, pg_cron, pg_hint_plan, pg_prewarm, pg_similarity, pg_stat_statements, pg_transport, and plprofiler.

8. Reboot the RDS for PostgreSQL DB instance so that your change to the `shared_preload_libraries` parameter takes effect.
9. When the instance is available, verify that pgAudit has been initialized. Use `psql` to connect to the RDS for PostgreSQL DB instance, and then run the following command.

```
SHOW shared_preload_libraries;
shared_preload_libraries
-----
rdsutils,pgaudit
(1 row)
```

10. With pgAudit initialized, you can now create the extension. You need to create the extension after initializing the library because the `pgaudit` extension installs event triggers for auditing data definition language (DDL) statements.

```
CREATE EXTENSION pgaudit;
```

11. Close the `psql` session.

```
labdb=> \q
```

12. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
13. Find the `pgaudit.log` parameter in the list and set to the appropriate value for your use case. For example, setting the `pgaudit.log` parameter to `write` as shown in the following image captures inserts, updates, deletes, and some other types changes to the log.

Name	Values	Allowed values	Modifiable
pgaudit.log	write	ddl, function, misc, read, role, write, none, all, -ddl, -function, -misc, -read, -role, -write	true

You can also choose one of the following values for the `pgaudit.log` parameter.

- `none` – This is the default. No database changes are logged.
- `all` – Logs everything (read, write, function, role, ddl, misc).
- `ddl` – Logs all data definition language (DDL) statements that aren't included in the ROLE class.
- `function` – Logs function calls and DO blocks.
- `misc` – Logs miscellaneous commands, such as DISCARD, FETCH, CHECKPOINT, VACUUM, and SET.
- `read` – Logs SELECT and COPY when the source is a relation (such as a table) or a query.
- `role` – Logs statements related to roles and privileges, such as GRANT, REVOKE, CREATE ROLE, ALTER ROLE, and DROP ROLE.
- `write` – Logs INSERT, UPDATE, DELETE, TRUNCATE, and COPY when the destination is a relation (table).

14. Choose **Save changes**.

15. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

16. Choose your RDS for PostgreSQL DB instance from the Databases list to select it, and then choose **Reboot** from the Actions menu.

AWS CLI

To setup pgAudit

To setup pgAudit using the AWS CLI, you call the `modify-db-parameter-group` operation to modify the audit log parameters in your custom parameter group, as shown in the following procedure.

1. Use the following AWS CLI command to add `pgaudit` to the `shared_preload_libraries` parameter.

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name custom-param-group-name \
  --parameters \
  "ParameterName=shared_preload_libraries,ParameterValue=pgaudit,ApplyMethod=pending-reboot" \
  --region aws-region
```

2. Use the following AWS CLI command to reboot the RDS for PostgreSQL DB instance so that the `pgaudit` library is initialized.

```
aws rds reboot-db-instance \
  --db-instance-identifier your-instance \
  --region aws-region
```

3. When the instance is available, you can verify that pgaudit has been initialized. Use psql to connect to the RDS for PostgreSQL DB instance, and then run the following command.

```
SHOW shared_preload_libraries;
shared_preload_libraries
-----
rdsutils,pgaudit
(1 row)
```

With pgAudit initialized, you can now create the extension.

```
CREATE EXTENSION pgaudit;
```

4. Close the psql session so that you can use the AWS CLI.

```
labdb=> \q
```

5. Use the following AWS CLI command to specify the classes of statement that want logged by session audit logging. The example sets the pgaudit.log parameter to `write`, which captures inserts, updates, and deletes to the log.

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name custom-param-group-name \
  --parameters "ParameterName=pgaudit.log,ParameterValue=write,ApplyMethod=pending-reboot" \
  --region aws-region
```

You can also choose one of the following values for the pgaudit.log parameter.

- `none` – This is the default. No database changes are logged.
- `all` – Logs everything (read, write, function, role, ddl, misc).
- `ddl` – Logs all data definition language (DDL) statements that aren't included in the `ROLE` class.
- `function` – Logs function calls and DO blocks.
- `misc` – Logs miscellaneous commands, such as `DISCARD`, `FETCH`, `CHECKPOINT`, `VACUUM`, and `SET`.
- `read` – Logs `SELECT` and `COPY` when the source is a relation (such as a table) or a query.
- `role` – Logs statements related to roles and privileges, such as `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE`, and `DROP ROLE`.
- `write` – Logs `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE`, and `COPY` when the destination is a relation (table).

Reboot the RDS for PostgreSQL DB instance using the following AWS CLI command.

```
aws rds reboot-db-instance \
  --db-instance-identifier your-instance \
  --region aws-region
```

Auditing database objects

With pgAudit set up on your RDS for PostgreSQL DB instance and configured for your requirements, more detailed information is captured in the PostgreSQL log. For example, while the default PostgreSQL logging configuration identifies the date and time that a change was made in a database table, with the pgAudit extension the log entry can include the schema, user who made the change, and other details

depending on how the extension parameters are configured. You can set up auditing to track changes in the following ways.

- For each session, by user. For the session level, you can capture the fully qualified command text.
- For each object, by user and by database.

The object auditing capability is activated when you create the `rds_pgaudit` role on your system and then add this role to the `pgaudit.role` parameter in your custom parameter parameter group. By default, the `pgaudit.role` parameter is unset and the only allowable value is `rds_pgaudit`. The following steps assume that `pgaudit` has been initialized and that you have created the `pgaudit` extension by following the procedure in [Setting up the pgAudit extension \(p. 1951\)](#).

```
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: statement: SELECT feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: AUDIT: SESSION,2,1,READ,SELECT,TABLE,public.support,"SELECT
feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC",none>
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: QUERY STATISTICS
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:DETAIL: ! system usage stats:
! 0.009494 s user, 0.007442 s system, 0.141985 s elapsed
! {0.022327 s user, 0.007442 s system total}
```

As shown in this example, the "LOG: AUDIT: SESSION" line provides information about the table and its schema, among other details.

To set up object auditing

1. Use `psql` to connect to the RDS for PostgreSQL DB instance.

```
psql --host=your-instance-name.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

2. Create a database role named `rds_pgaudit` using the following command.

```
labdb=> CREATE ROLE rds_pgaudit;
CREATE ROLE
labdb=>
```

3. Close the `psql` session.

```
labdb=> \q
```

In the next few steps, use the AWS CLI to modify the audit log parameters in your custom parameter group.

4. Use the following AWS CLI command to set the `pgaudit.role` parameter to `rds_pgaudit`. By default, this parameter is empty, and `rds_pgaudit` is the only allowable value.

```
aws rds modify-db-parameter-group \
--db-parameter-group-name custom-param-group-name \
--parameters
"ParameterName=pgaudit.role,ParameterValue=rds_pgaudit,ApplyMethod=pending-reboot" \
--region aws-region
```

5. Use the following AWS CLI command to reboot the RDS for PostgreSQL DB instance so that your changes to the parameters take effect.

```
aws rds reboot-db-instance \
--db-instance-identifier your-instance \
--region aws-region
```

6. Run the following command to confirm that the `pgaudit.role` is set to `rds_pgaudit`.

```
SHOW pgaudit.role;
pgaudit.role
-----
rds_pgaudit
```

To test pgAudit logging, you can run several example commands that you want to audit. For example, you might run the following commands.

```
CREATE TABLE t1 (id int);
GRANT SELECT ON t1 TO rds_pgaudit;
SELECT * FROM t1;
id
-----
(0 rows)
```

The database logs should contain an entry similar to the following.

```
...
2017-06-12 19:09:49 UTC:...:rds_test@postgres:[11701]:LOG: AUDIT:
OBJECT,1,1,READ,SELECT,TABLE,public.t1,select * from t1;
...
```

For information on viewing the logs, see [Monitoring Amazon RDS log files \(p. 680\)](#).

To learn more about the pgAudit extension, see [pgAudit](#) on GitHub.

Excluding users or databases from audit logging

As discussed in [RDS for PostgreSQL database log files \(p. 716\)](#), PostgreSQL logs consume storage space. Using the pgAudit extension adds to the volume of data gathered in your logs to varying degrees, depending on the changes that you track. You might not need to audit every user or database in your RDS for PostgreSQL DB instance.

To minimize impacts to your storage and to avoid needlessly capturing audit records, you can exclude users and databases from being audited. You can also change logging within a given session. The following examples show you how.

Note

Parameter settings at the session level take precedence over the settings in the custom DB parameter group for the RDS for PostgreSQL DB instance. If you don't want database users to bypass your audit logging configuration settings, be sure to change their permissions.

Suppose that your RDS for PostgreSQL DB instance is configured to audit the same level of activity for all users and databases. You then decide that you don't want to audit the user `myuser`. You can turn off auditing for `myuser` with the following SQL command.

```
ALTER USER myuser SET pgaudit.log TO 'NONE';
```

Then, you can use the following query to check the `user_specific_settings` column for `pgaudit.log` to confirm that the parameter is set to `NONE`.

```
SELECT
    username AS user_name,
    useconfig AS user_specific_settings
```

```
FROM
    pg_user
WHERE
    username = 'myuser';
```

You see output such as the following.

user_name	user_specific_settings
myuser	{pgaudit.log=NONE}

(1 row)

You can turn off logging for a given user in the midst of their session with the database with the following command.

```
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'none';
```

Use the following query to check the settings column for pgaudit.log for a specific user and database combination.

```
SELECT
    username AS "user_name",
    datname AS "database_name",
    pg_catalog.array_to_string(setconfig, E'\n') AS "settings"
FROM
    pg_catalog.pg_db_role_setting s
    LEFT JOIN pg_catalog.pg_database d ON d.oid = setdatabase
    LEFT JOIN pg_catalog.pg_user r ON r.usesysid = setrole
WHERE
    username = 'myuser'
    AND datname = 'mydatabase'
ORDER BY
    1,
    2;
```

You see output similar to the following.

user_name	database_name	settings
myuser	mydatabase	pgaudit.log=none

(1 row)

After turning off auditing for myuser, you decide that you don't want to track changes to mydatabase. You turn off auditing for that specific database by using the following command.

```
ALTER DATABASE mydatabase SET pgaudit.log to 'NONE';
```

Then, use the following query to check the database_specific_settings column to confirm that pgaudit.log is set to NONE.

```
SELECT
    a.datname AS database_name,
    b.setconfig AS database_specific_settings
FROM
    pg_database a
    FULL JOIN pg_db_role_setting b ON a.oid = b.setdatabase
WHERE
```

```
a.datname = 'mydatabase';
```

You see output such as the following.

```
database_name | database_specific_settings
-----+-----
mydatabase    | {pgaudit.log=NONE}
(1 row)
```

To return settings to the default setting for myuser, use the following command:

```
ALTER USER myuser RESET pgaudit.log;
```

To return settings to their default setting for a database, use the following command.

```
ALTER DATABASE mydatabase RESET pgaudit.log;
```

To reset user and database to the default setting, use the following command.

```
ALTER USER myuser IN DATABASE mydatabase RESET pgaudit.log;
```

You can also capture specific events to the log by setting the `pgaudit.log` to one of the other allowed values for the `pgaudit.log` parameter. For more information, see [List of allowable settings for the `pgaudit.log` parameter \(p. 1959\)](#).

```
ALTER USER myuser SET pgaudit.log TO 'read';
ALTER DATABASE mydatabase SET pgaudit.log TO 'function';
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'read,function'
```

Reference for the pgAudit extension

You can specify the level of detail that you want for your audit log by changing one or more of the parameters listed in this section.

Controlling pgAudit behavior

You can control the audit logging by changing one or more of the parameters listed in the following table.

Parameter	Description
<code>pgaudit.log</code>	Specifies the statement classes that will be logged by session audit logging. Allowable values include <code>ddl</code> , <code>function</code> , <code>misc</code> , <code>read</code> , <code>role</code> , <code>write</code> , <code>none</code> , <code>all</code> . For more information, see List of allowable settings for the <code>pgaudit.log</code> parameter (p. 1959) .
<code>pgaudit.log_catalog</code>	When turned on (set to 1), adds statements to audit trail if all relations in a statement are in <code>pg_catalog</code> .
<code>pgaudit.log_level</code>	Specifies the log level to use for log entries. Allowed values: <code>debug5</code> , <code>debug4</code> , <code>debug3</code> , <code>debug2</code> , <code>debug1</code> , <code>info</code> , <code>notice</code> , <code>warning</code> , <code>log</code>
<code>pgaudit.log_parameter</code>	When turned on (set to 1), parameters passed with the statement are captured in the audit log.

Parameter	Description
<code>pgaudit.log_relation</code>	When turned on (set to 1), the audit log for the session creates a separate log entry for each relation (TABLE, VIEW, and so on) referenced in a SELECT or DML statement.
<code>pgaudit.log_statement_once</code>	Specifies whether logging will include the statement text and parameters with the first log entry for a statement/substatement combination or with every entry.
<code>pgaudit.role</code>	Specifies the master role to use for object audit logging. The only allowable entry is <code>rds_pgaudit</code> .

List of allowable settings for the `pgaudit.log` parameter

Value	Description
<code>none</code>	This is the default. No database changes are logged.
<code>all</code>	Logs everything (read, write, function, role, ddl, misc).
<code>ddl</code>	Logs all data definition language (DDL) statements that aren't included in the ROLE class.
<code>function</code>	Logs function calls and DO blocks.
<code>misc</code>	Logs miscellaneous commands, such as DISCARD, FETCH, CHECKPOINT, VACUUM, and SET.
<code>read</code>	Logs SELECT and COPY when the source is a relation (such as a table) or a query.
<code>role</code>	Logs statements related to roles and privileges, such as GRANT, REVOKE, CREATE ROLE, ALTER ROLE, and DROP ROLE.
<code>write</code>	Logs INSERT, UPDATE, DELETE, TRUNCATE, and COPY when the destination is a relation (table).

To log multiple event types with session auditing, use a comma-separated list. To log all event types, set `pgaudit.log` to ALL. Reboot your DB instance to apply the changes.

With object auditing, you can refine audit logging to work with specific relations. For example, you can specify that you want audit logging for READ operations on one or more tables.

Scheduling maintenance with the PostgreSQL pg_cron extension

You can use the PostgreSQL pg_cron extension to schedule maintenance commands within a PostgreSQL database. For more information about the extension, see [What is pg_cron?](#) in the pg_cron documentation.

The pg_cron extension is supported on RDS for PostgreSQL engine versions 12.5 and higher.

To learn more about using pg_cron, see [Schedule jobs with pg_cron on your RDS for PostgreSQL or your Aurora PostgreSQL-Compatible Edition databases](#)

Topics

- [Setting up the pg_cron extension \(p. 1960\)](#)
- [Granting database users permissions to use pg_cron \(p. 1960\)](#)
- [Scheduling pg_cron jobs \(p. 1961\)](#)
- [Reference for the pg_cron extension \(p. 1963\)](#)

Setting up the pg_cron extension

Set up the pg_cron extension as follows:

1. Modify the custom parameter group associated with your PostgreSQL DB instance by adding pg_cron to the shared_preload_libraries parameter value.
 - If your RDS for PostgreSQL DB instance uses the rds.allowed_extensions parameter to explicitly list extensions that can be installed, you need to add the pg_cron extension to the list. Only certain versions of RDS for PostgreSQL support the rds.allowed_extensions parameter. By default, all available extensions are allowed. For more information, see [Restricting installation of PostgreSQL extensions \(p. 1807\)](#).

Restart the PostgreSQL DB instance to have changes to the parameter group take effect. To learn more about working with parameter groups, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

2. After the PostgreSQL DB instance has restarted, run the following command using an account that has rds_superuser permissions. For example, if you used the default settings when you created your RDS for PostgreSQL DB instance, connect as user postgres and create the extension.

```
CREATE EXTENSION pg_cron;
```

The pg_cron scheduler is set in the default PostgreSQL database named postgres. The pg_cron objects are created in this postgres database and all scheduling actions run in this database.

3. You can use the default settings, or you can schedule jobs to run in other databases within your PostgreSQL DB instance. To schedule jobs for other databases within your PostgreSQL DB instance, see the example in [Scheduling a cron job for a database other than postgres \(p. 1962\)](#).

Granting database users permissions to use pg_cron

Installing the pg_cron extension requires the rds_superuser privileges. However, permissions to use the pg_cron can be granted (by a member of the rds_superuser group/role) to other database users, so that they can schedule their own jobs. We recommend that you grant permissions to the cron schema only as needed if it improves operations in your production environment.

To grant a database user permission in the `cron` schema, run the following command:

```
postgres=> GRANT USAGE ON SCHEMA cron TO db-user;
```

This gives `db-user` permission to access the `cron` schema to schedule cron jobs for the objects that they have permissions to access. If the database user doesn't have permissions, the job fails after posting the error message to the `postgresql.log` file, as shown in the following:

```
2020-12-08 16:41:00 UTC::@:[30647]:ERROR: permission denied for table table-name
2020-12-08 16:41:00 UTC::@:[27071]:LOG: background worker "pg_cron" (PID 30647) exited with
exit code 1
```

IN other words, make sure that database users that are granted permissions on the cron schema also have permissions on the objects (tables, schemas, and so on) that they plan to schedule.

The details of the cron job and its success or failure are also captured in the `cron.job_run_details` table. For more information, see [Tables for scheduling jobs and capturing status \(p. 1965\)](#).

Scheduling pg_cron jobs

The following sections show how you can schedule various management tasks using `pg_cron` jobs.

Note

Note
When you create pg_cron jobs, check that the max_worker_processes setting is larger than the number of cron.max_running_jobs. A pg_cron job fails if it runs out of background worker processes. The default number of pg_cron jobs is 5. For more information, see [Parameters for managing the pg_cron extension \(p. 1963\)](#).

Topics

- Vacuuming a table (p. 1961)
 - Purging the pg_cron history table (p. 1962)
 - Logging errors to the postgresql.log file only (p. 1962)
 - Scheduling a cron job for a database other than postgres (p. 1962)

Vacuuming a table

Autovacuum handles vacuum maintenance for most cases. However, you might want to schedule a vacuum of a specific table at a time of your choosing.

See also: [Working with the PostgreSQL autovacuum on Amazon RDS for PostgreSQL](#) (p. 1924).

Following is an example of using the `cron.schedule` function to set up a job to use VACUUM FREEZE on a specific table every day at 22:00 (GMT).

```
SELECT cron.schedule('manual vacuum', '0 22 * * *', 'VACUUM FREEZE pgbench_accounts');
schedule
-----
1
(1 row)
```

After the preceding example runs, you can check the history in the `cron.job_run_details` table as follows.

```
postgres=> SELECT * FROM cron.job_run_details;
jobid | runid | job_pid | database | username | command
      |       |          |          |          |          | status
      |       |          |          |          |          |
      |       |          |          |          |          | end_time
```

jobid	runid	start_time	end_time	database	username	command	status
1	1	2020-12-04 21:10:00.050386+00	2020-12-04 21:10:00.072028+00	postgres	adminuser	vacuum freeze pgbench_accounts	succeeded

Following is an querying the cron.job_run_details table to see failed jobs.

jobid	runid	start_time	end_time	database	username	command	status
5	4	2020-12-04 21:48:00.029567+00	2020-12-04 21:48:00.015145+00	postgres	adminuser	vacuum freeze pgbench_account	failed

For more information, see [Tables for scheduling jobs and capturing status \(p. 1965\)](#).

Purging the pg_cron history table

The cron.job_run_details table contains a history of cron jobs that can become very large over time. We recommend that you schedule a job that purges this table. For example, keeping a week's worth of entries might be sufficient for troubleshooting purposes.

The following example uses the [cron.schedule \(p. 1964\)](#) function to schedule a job that runs every day at midnight to purge the cron.job_run_details table. The job keeps only the last seven days. Use your rds_superuser account to schedule the job such as the following.

```
SELECT cron.schedule('0 0 * * *', $$DELETE
    FROM cron.job_run_details
    WHERE end_time < now() - interval '7 days$$);
```

For more information, see [Tables for scheduling jobs and capturing status \(p. 1965\)](#).

Logging errors to the postgresql.log file only

To prevent writing to the cron.job_run_details table, modify the parameter group associated with the PostgreSQL DB instance and set the cron.log_run parameter to off. The pg_cron extension no longer writes to the table and captures errors to the postgresql.log file only. For more information, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Use the following command to check the value of the cron.log_run parameter.

```
postgres=> SHOW cron.log_run;
```

For more information, see [Parameters for managing the pg_cron extension \(p. 1963\)](#).

Scheduling a cron job for a database other than postgres

The metadata for pg_cron is all held in the PostgreSQL default database named postgres. Because background workers are used for running the maintenance cron jobs, you can schedule a job in any of your databases within the PostgreSQL DB instance:

1. In the cron database, schedule the job as you normally do using the [cron.schedule \(p. 1964\)](#).

```
postgres=> SELECT cron.schedule('database1 manual vacuum', '29 03 * * *', 'vacuum freeze test_table');
```

2. As a user with the `rds_superuser` role, update the database column for the job that you just created so that it runs in another database within your PostgreSQL DB instance.

```
postgres=> UPDATE cron.job SET database = 'database1' WHERE jobid = 106;
```

3. Verify by querying the `cron.job` table.

```
postgres=> SELECT * FROM cron.job;
   jobid | schedule      | command                                | nodename | nodeport | database |
   username | active | jobname
-----+-----+-----+-----+-----+-----+
106    | 29 03 * * * | vacuum freeze test_table      | localhost | 8192     | database1|
adminuser | t      | database1 manual vacuum          |           |           |           |
1       | 59 23 * * * | vacuum freeze pgbench_accounts | localhost | 8192     | postgres  |
adminuser | t      | manual vacuum                   |           |           |           |
(2 rows)
```

Note

In some situations, you might add a cron job that you intend to run on a different database. In such cases, the job might try to run in the default database (`postgres`) before you update the correct database column. If the user name has permissions, the job successfully runs in the default database.

Reference for the pg_cron extension

You can use the following parameters, functions, and tables with the pg_cron extension. For more information, see [What is pg_cron?](#) in the pg_cron documentation.

Topics

- [Parameters for managing the pg_cron extension \(p. 1963\)](#)
- [Function reference: cron.schedule \(p. 1964\)](#)
- [Function reference: cron.unschedule \(p. 1965\)](#)
- [Tables for scheduling jobs and capturing status \(p. 1965\)](#)

Parameters for managing the pg_cron extension

Following is a list of parameters that control the pg_cron extension behavior.

Parameter	Description
<code>cron.database_name</code>	The database in which pg_cron metadata is kept.
<code>cron.host</code>	The hostname to connect to PostgreSQL. You can't modify this value.
<code>cron.log_run</code>	Log every job that runs in the <code>job_run_details</code> table. Values are on or off. For more information, see Tables for scheduling jobs and capturing status (p. 1965) .

Parameter	Description
cron.log_statement	Log all cron statements before running them. Values are on or off.
cron.max_running_jobs	The maximum number of jobs that can run concurrently.
cron.use_background_workers	Use background workers instead of client sessions. You can't modify this value.

Use the following SQL command to display these parameters and their values.

```
postgres=> SELECT name, setting, short_desc FROM pg_settings WHERE name LIKE 'cron.%' ORDER BY name;
```

Function reference: cron.schedule

This function schedules a cron job. The job is initially scheduled in the default `postgres` database. The function returns a bigint value representing the job identifier. To schedule jobs to run in other databases within your PostgreSQL DB instance, see the example in [Scheduling a cron job for a database other than postgres \(p. 1962\)](#).

The function has two syntax formats.

Syntax

```
cron.schedule (job_name,
               schedule,
               command
               );
cron.schedule (schedule,
               command
               );
```

Parameters

Parameter	Description
job_name	The name of the cron job.
schedule	Text indicating the schedule for the cron job. The format is the standard cron format.
command	Text of the command to run.

Examples

```
postgres=> SELECT cron.schedule ('test','0 10 * * *', 'VACUUM pgbench_history');
          schedule
          -----
                  145
(1 row)
```

```
postgres=> SELECT cron.schedule ('0 15 * * *', 'VACUUM pgbench_accounts');
schedule
-----
146
(1 row)
```

Function reference: cron.unschedule

This function deletes a cron job. You can specify either the `job_name` or the `job_id`. A policy makes sure that you are the owner to remove the schedule for the job. The function returns a Boolean indicating success or failure.

The function has the following syntax formats.

Syntax

```
cron.unschedule (job_id);
cron.unschedule (job_name);
```

Parameters

Parameter	Description
<code>job_id</code>	A job identifier that was returned from the <code>cron.schedule</code> function when the cron job was scheduled.
<code>job_name</code>	The name of a cron job that was scheduled with the <code>cron.schedule</code> function.

Examples

```
postgres=> SELECT cron.unschedule(108);
unschedule
-----
t
(1 row)

postgres=> SELECT cron.unschedule('test');
unschedule
-----
t
(1 row)
```

Tables for scheduling jobs and capturing status

The following tables are used to schedule the cron jobs and record how the jobs completed.

Table	Description
<code>cron.job</code>	Contains the metadata about each scheduled job. Most interactions with this table should be done by using the <code>cron.schedule</code> and <code>cron.unschedule</code> functions.

Table	Description
	<p>Important We recommend that you don't give update or insert privileges directly to this table. Doing so would allow the user to update the username column to run as rds-superuser.</p>
cron.job_run_details	<p>Contains historic information about past scheduled jobs that ran. This is useful to investigate the status, return messages, and start and end time from the job that ran.</p> <p>Note To prevent this table from growing indefinitely, purge it on a regular basis. For an example, see Purging the pg_cron history table (p. 1962).</p>

Using pglogical to synchronize data across instances

All currently available RDS for PostgreSQL versions support the pglogical extension. The pglogical extension predates the functionally similar logical replication feature that was introduced by PostgreSQL in version 10. For more information, see [Performing logical replication for Amazon RDS for PostgreSQL \(p. 1908\)](#).

The pglogical extension supports logical replication between two or more RDS for PostgreSQL DB instances. It also supports replication between different PostgreSQL versions, and between databases running on RDS for PostgreSQL DB instances and Aurora PostgreSQL DB clusters. The pglogical extension uses a publish-subscribe model to replicate changes to tables and other objects, such as sequences, from a publisher to a subscriber. It relies on a replication slot to ensure that changes are synchronized from a publisher node to a subscriber node, defined as follows.

- The *publisher node* is the RDS for PostgreSQL DB instance that's the source of data to be replicated to other nodes. The publisher node defines the tables to be replicated in a publication set.
- The *subscriber node* is the RDS for PostgreSQL DB instance that receives WAL updates from the publisher. The subscriber creates a subscription to connect to the publisher and get the decoded WAL data. When the subscriber creates the subscription, the replication slot is created on the publisher node.

Following, you can find information about setting up the pglogical extension.

Topics

- [Requirements and limitations for the pglogical extension \(p. 1967\)](#)
- [Setting up the pglogical extension \(p. 1967\)](#)
- [Setting up logical replication for RDS for PostgreSQL DB instance \(p. 1970\)](#)
- [Reestablishing logical replication after a major upgrade \(p. 1972\)](#)
- [Managing logical replication slots for RDS for PostgreSQL \(p. 1974\)](#)
- [Parameter reference for the pglogical extension \(p. 1975\)](#)

Requirements and limitations for the pglogical extension

All currently available releases of RDS for PostgreSQL support the pglogical extension.

Both the publisher node and the subscriber node must be set up for logical replication.

The tables that you want to replicate from subscriber to publisher must have the same names and the same schema. These tables must also contain the same columns, and the columns must use the same data types. Both publisher and subscriber tables must have the same primary keys. We recommend that you use only the PRIMARY KEY as the unique constraint.

The tables on the subscriber node can have more permissive constraints than those on the publisher node for CHECK constraints and NOT NULL constraints.

The pglogical extension provides features such as two-way replication that aren't supported by the logical replication feature built into PostgreSQL (version 10 and higher). For more information, see [PostgreSQL bi-directional replication using pglogical](#).

Setting up the pglogical extension

To set up the pglogical extension on your RDS for PostgreSQL DB instance , you add pglogical to the shared libraries on the custom DB parameter group for your RDS for PostgreSQL DB instance.

You also need to set the value of the `rds.logical_replication` parameter to 1, to turn on logical decoding. Finally, you create the extension in the database. You can use the AWS Management Console or the AWS CLI for these tasks.

You must have permissions as the `rds_superuser` role to perform these tasks.

The steps following assume that your RDS for PostgreSQL DB instance is associated with a custom DB parameter group. For information about creating a custom DB parameter group, see [Working with parameter groups \(p. 289\)](#).

Console

To set up the pglogical extension

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose your RDS for PostgreSQL DB instance.
3. Open the **Configuration** tab for your RDS for PostgreSQL DB instance. Among the Instance details, find the **Parameter group** link.
4. Choose the link to open the custom parameters associated with your RDS for PostgreSQL DB instance.
5. In the **Parameters** search field, type `shared_pre` to find the `shared_preload_libraries` parameter.
6. Choose **Edit parameters** to access the property values.
7. Add `pglogical` to the list in the **Values** field. Use a comma to separate items in the list of values.

The screenshot shows the AWS RDS Parameter Groups page. The URL is [RDS > Parameter groups > docs-lab-rpg-12-parameter-group](#). The page title is "docs-lab-rpg-12-parameter-group". Under the "Parameters" section, there is a search bar containing "shared_pre". A table lists the parameter "shared_preload_libraries" with the value "pglogical,pg_stat_statements". To the right of the value, a tooltip shows the allowed values: "auto_explain, orafce, pgaudit, pglogical, pg_bigm, pg_cron, pg_hint_plan, pg_prewarm, pg_similarity, pg_stat_statements, pg_transport, plprofiler".

8. Find the `rds.logical_replication` parameter and set it to 1, to turn on logical replication.
9. Reboot the RDS for PostgreSQL DB instance so that your changes take effect.
10. When the instance is available, you can use `psql` (or `pgAdmin`) to connect to the RDS for PostgreSQL DB instance.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres  
--password --dbname=labdb
```

11. To verify that pglogical is initialized, run the following command.

```
SHOW shared_preload_libraries;  
shared_preload_libraries  
-----  
rdsutils,pglogical
```

```
(1 row)
```

12. Verify the setting that enables logical decoding, as follows.

```
SHOW wal_level;
wal_level
-----
logical
(1 row)
```

13. Create the extension, as follows.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

14. Choose **Save changes**.

15. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

16. Choose your RDS for PostgreSQL DB instance from the Databases list to select it, and then choose **Reboot** from the Actions menu.

AWS CLI

To setup the pglogical extension

To setup pglogical using the AWS CLI, you call the [modify-db-parameter-group](#) operation to modify certain parameters in your custom parameter group as shown in the following procedure.

1. Use the following AWS CLI command to add pglogical to the shared_preload_libraries parameter.

```
aws rds modify-db-parameter-group \
--db-parameter-group-name custom-param-group-name \
--parameters \
"ParameterName=shared_preload_libraries,ParameterValue=pglogical,ApplyMethod=pending-reboot" \
--region aws-region
```

2. Use the following AWS CLI command to set rds.logical_replication to 1 to turn on the logical decoding capability for the RDS for PostgreSQL DB instance.

```
aws rds modify-db-parameter-group \
--db-parameter-group-name custom-param-group-name \
--parameters \
"ParameterName=rds.logical_replication,ParameterValue=1,ApplyMethod=pending-reboot" \
--region aws-region
```

3. Use the following AWS CLI command to reboot the RDS for PostgreSQL DB instance so that the pglogical library is initialized.

```
aws rds reboot-db-instance \
--db-instance-identifier your-instance \
--region aws-region
```

4. When the instance is available, use psql to connect to the RDS for PostgreSQL DB instance.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres \
--password --dbname=labdb
```

5. Create the extension, as follows.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

6. Reboot the RDS for PostgreSQL DB instance using the following AWS CLI command.

```
aws rds reboot-db-instance \
--db-instance-identifier your-instance \
--region aws-region
```

Setting up logical replication for RDS for PostgreSQL DB instance

The following procedure shows you how to start logical replication between two RDS for PostgreSQL DB instances. The steps assume that both the source (publisher) and the target (subscriber) have the pglogical extension set up as detailed in [Setting up the pglogical extension \(p. 1967\)](#).

To create the publisher node and define the tables to replicate

These steps assume that your RDS for PostgreSQL DB instance has a database that has one or more tables that you want to replicate to another node. You need to recreate the table structure from the publisher on the subscriber, so first, get the table structure if necessary. You can do that by using the psql metacommand `\d tablename` and then creating the same table on the subscriber instance. The following procedure creates an example table on the publisher (source) for demonstration purposes.

1. Use psql to connect to the instance that has the table you want to use as a source for subscribers.

```
psql --host=source-instance.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

If you don't have an existing table that you want to replicate, you can create a sample table as follows.

- a. Create an example table using the following SQL statement.

```
CREATE TABLE docs_lab_table (a int PRIMARY KEY);
```

- b. Populate the table with generated data by using the following SQL statement.

```
INSERT INTO docs_lab_table VALUES (generate_series(1,5000));
INSERT 0 5000
```

- c. Verify that data exists in the table by using the following SQL statement.

```
SELECT count(*) FROM docs_lab_table;
```

2. Identify this RDS for PostgreSQL DB instance as the publisher node, as follows.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_provider',
    dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432 dbname=labdb');
create_node
-----
3410995529
(1 row)
```

3. Add the table that you want to replicate to the default replication set. For more information about replication sets, see [Replication sets](#) in the pglogical documentation.

```
SELECT pglogical.replication_set_add_table('default', 'docs_lab_table', 'true', NULL,
NULL);
replication_set_add_table
-----
t
(1 row)
```

The publisher node setup is complete. You can now set up the subscriber node to receive the updates from the publisher.

To set up the subscriber node and create a subscription to receive updates

These steps assume that the RDS for PostgreSQL DB instance has been set up with the pglogical extension. For more information, see [Setting up the pglogical extension \(p. 1967\)](#).

1. Use psql to connect to the instance that you want to receive updates from the publisher.

```
psql --host=target-instance.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

2. On the subscriber RDS for PostgreSQL DB instance, create the same table that exists on the publisher. For this example, the table is docs_lab_table. You can create the table as follows.

```
CREATE TABLE docs_lab_table (a int PRIMARY KEY);
```

3. Verify that this table is empty.

```
SELECT count(*) FROM docs_lab_table;
count
-----
0
(1 row)
```

4. Identify this RDS for PostgreSQL DB instance as the subscriber node, as follows.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_target',
    dsn := 'host=target-instance.aws-region.rds.amazonaws.com port=5432 sslmode=require
dbname=labdb user=postgres password=*****');
create_node
-----
2182738256
(1 row)
```

5. Create the subscription.

```
SELECT pglogical.create_subscription(
    subscription_name := 'docs_lab_subscription',
    provider_dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432
sslmode=require dbname=labdb user=postgres password=*****',
    replication_sets := ARRAY['default'],
    synchronize_data := true,
    forward_origins := '{}');
create_subscription
-----
1038357190
```

(1 row)

When you complete this step, the data from the table on the publisher is created in the table on the subscriber. You can verify that this has occurred by using the following SQL query.

```
SELECT count(*) FROM docs_lab_table;
count
-----
 5000
(1 row)
```

From this point forward, changes made to the table on the publisher are replicated to the table on the subscriber.

Reestablishing logical replication after a major upgrade

Before you can perform a major version upgrade of an RDS for PostgreSQL DB instance that's set up as a publisher node for logical replication, you must drop all replication slots, even those that aren't active. We recommend that you temporarily divert database transactions from the publisher node, drop the replication slots, upgrade the RDS for PostgreSQL DB instance, and then re-establish and restart replication.

The replication slots are hosted on the publisher node only. The RDS for PostgreSQL subscriber node in a logical replication scenario has no slots to drops, but it can't be upgraded to a major version while it's designated as a subscriber node with a subscription to the publisher. Before upgrading the RDS for PostgreSQL subscriber node, drop the subscription and the node. For more information, see [Managing logical replication slots for RDS for PostgreSQL \(p. 1974\)](#).

Determining that logical replication has been disrupted

You can determine that the replication process has been disrupted by querying either the publisher node or the subscriber node, as follows.

To check the publisher node

- Use `psql` to connect to the publisher node, and then query the `pg_replication_slots` function. Note the value in the `active` column. Normally, this will return `t` (true), showing that replication is active. If the query returns `f` (false), it's an indication that replication to the subscriber has stopped.

```
SELECT slot_name,plugin,slot_type,active FROM pg_replication_slots;
slot_name          |    plugin    | slot_type | active
-----+-----+-----+-----+
pgl_labdb_docs_labcb4fa94_docs_lab3de412c | pglogical_output | logical   | f
(1 row)
```

To check the subscriber node

On the subscriber node, you can check the status of replication in three different ways.

- Look through the PostgreSQL logs on the subscriber node to find failure messages. The log identifies failure with messages that include exit code 1, as shown following.

```
2022-07-06 16:17:03 UTC::@[7361]:LOG: background worker "pglogical apply
16404:2880255011" (PID 14610) exited with exit code 1
2022-07-06 16:19:44 UTC::@[7361]:LOG: background worker "pglogical apply
16404:2880255011" (PID 21783) exited with exit code 1
```

- Query the `pg_replication_origin` function. Connect to the database on the subscriber node using `psql` and query the `pg_replication_origin` function, as follows.

```
SELECT * FROM pg_replication_origin;
roident | roname
-----+-----
(0 rows)
```

The empty result set means that replication has been disrupted. Normally, you see output such as the following.

```
roident | roname
-----+-----
1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

- Query the `pglogical.show_subscription_status` function as shown in the following example.

```
SELECT subscription_name,status,slot_name FROM pglogical.show_subscription_status();
subscription_name | status | slot_name
-----+-----+-----
docs_lab_subscription | down | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

This output shows that replication has been disrupted. Its status is down. Normally, the output shows the status as replicating.

If your logical replication process has been disrupted, you can re-establish replication by following these steps.

To reestablish logical replication between publisher and subscriber nodes

To re-establish replication, you first disconnect the subscriber from the publisher node and then re-establish the subscription, as outlined in these steps.

1. Connect to the subscriber node using `psql` as follows.

```
psql --host=2222222222.aws-region.rds.amazonaws.com --port=5432 --username=postgres
--password --dbname=labdb
```

2. Deactivate the subscription by using the `pglogical.alter_subscription_disable` function.

```
SELECT pglogical.alter_subscription_disable('docs_lab_subscription',true);
alter_subscription_disable
-----
t
(1 row)
```

3. Get the publisher node's identifier by querying the `pg_replication_origin`, as follows.

```
SELECT * FROM pg_replication_origin;
roident | roname
-----+-----
1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

4. Use the response from the previous step with the `pg_replication_origin_create` command to assign the identifier that can be used by the subscription when re-established.

```
SELECT pg_replication_origin_create('pgl_labdb_docs_labcb4fa94_docs_lab3de412c');
    pg_replication_origin_create
-----
1
(1 row)
```

- Turn on the subscription by passing its name with a status of `true`, as shown in the following example.

```
SELECT pglogical.alter_subscription_enable('docs_lab_subscription',true);
    alter_subscription_enable
-----
t
(1 row)
```

Check the status of the node. Its status should be `replicating` as shown in this example.

```
SELECT subscription_name,status,slot_name
  FROM pglogical.show_subscription_status();
      subscription_name |   status   |           slot_name
-----
docs_lab_subscription | replicating | pgl_labdb_docs_lab98f517b_docs_lab3de412c
(1 row)
```

Check the status of the subscriber's replication slot on the publisher node. The slot's `active` column should return `t` (`true`), indicating that replication has been re-established.

```
SELECT slot_name,plugin,slot_type,active
  FROM pg_replication_slots;
      slot_name |     plugin     | slot_type | active
-----
pgl_labdb_docs_lab98f517b_docs_lab3de412c | pglogical_output | logical   | t
(1 row)
```

Managing logical replication slots for RDS for PostgreSQL

Before you can perform a major version upgrade on an RDS for PostgreSQL DB instance that's serving as a publisher node in a logical replication scenario, you must drop the replication slots on the instance. The major version upgrade pre-check process notifies you that the upgrade can't proceed until the slots are dropped.

To drop slots from your RDS for PostgreSQL DB instance, first drop the subscription and then drop the slot.

To identify replication slots that were created using the `pglogical` extension, log in to each database and get the name of the nodes. When you query the subscriber node, you get both the publisher and the subscriber nodes in the output, as shown in this example.

```
SELECT * FROM pglogical.node;
node_id | node_name
-----
2182738256 | docs_lab_target
3410995529 | docs_lab_provider
(2 rows)
```

You can get the details about the subscription with the following query.

```
SELECT sub_name,sub_slot_name,sub_target
  FROM pglogical.subscription;
  sub_name |      sub_slot_name      | sub_target
-----+-----+
docs_lab_subscription | pgl_labdb_docs_1abcb4fa94_docs_lab3de412c | 2182738256
(1 row)
```

You can now drop the subscription, as follows.

```
SELECT pglogical.drop_subscription(subscription_name := 'docs_lab_subscription');
drop_subscription
-----
1
(1 row)
```

After dropping the subscription, you can delete the node.

```
SELECT pglogical.drop_node(node_name := 'docs-lab-subscriber');
drop_node
-----
t
(1 row)
```

You can verify that the node no longer exists, as follows.

```
SELECT * FROM pglogical.node;
node_id | node_name
-----+-----
(0 rows)
```

Parameter reference for the pglogical extension

In the table you can find parameters associated with the pglogical extension. Parameters such as pglogical.conflict_log_level and pglogical.conflict_resolution are used to handle update conflicts. Conflicts can emerge when changes are made locally to the same tables that are subscribed to changes from the publisher. Conflicts can also occur during various scenarios, such as two-way replication or when multiple subscribers are replicating from the same publisher. For more information, see [PostgreSQL bi-directional replication using pglogical](#).

Parameter	Description
pglogical.batch_inserts	Batch inserts if possible. Not set by default. Change to '1' to turn on, '0' to turn off.
pglogical.conflict_log_level	Sets the log level to use for logging resolved conflicts. Supported string values are debug5, debug4, debug3, debug2, debug1, info, notice, warning, error, log, fatal, panic.
pglogical.conflict_resolution	Sets method to use to resolve conflicts when conflicts are resolvable. Supported string values are error, apply_remote, keep_local, last_update_wins, first_update_wins.
pglogical.extra_connection_options	Connection options to add to all peer node connections.
pglogical.synchronous_commit	pglogical specific synchronous commit value

Parameter	Description
pglogical.use_spi	Use SPI (server programming interface) instead of low-level API to apply changes. Set to '1' to turn on, '0' to turn off. For more information about SPI, see Server Programming Interface in the PostgreSQL documentation.

Reducing bloat in tables and indexes with the pg_repack extension

You can use the pg_repack extension to remove bloat from tables and indexes. This extension is supported on RDS for PostgreSQL versions 9.6.3 and higher. For more information on the pg_repack extension, see the [GitHub project documentation](#).

To use the pg_repack extension

1. Install the pg_repack extension on your RDS for PostgreSQL DB instance by running the following command.

```
CREATE EXTENSION pg_repack;
```

2. Run the following commands to grant write access to repack temporary log tables created by pg_repack.

```
ALTER DEFAULT PRIVILEGES IN SCHEMA repack GRANT INSERT ON TABLES TO PUBLIC;  
ALTER DEFAULT PRIVILEGES IN SCHEMA repack GRANT USAGE, SELECT ON SEQUENCES TO PUBLIC;
```

3. Connect to the database using the pg_repack client utility. Use an account that has rds_superuser privileges. As an example, assume that rds_test role has rds_superuser privileges. The command syntax is shown following.

```
pg_repack -h db-instance-name.111122223333.aws-region.rds.amazonaws.com -U rds_test -k  
postgres
```

Connect using the -k option. The -a option is not supported.

4. The response from the pg_repack client provides information on the tables on the DB instance that are repacked.

```
INFO: repacking table "pgbench_tellers"  
INFO: repacking table "pgbench_accounts"  
INFO: repacking table "pgbench_branches"
```

Upgrading and using the PLV8 extension

PLV8 is a trusted Javascript language extension for PostgreSQL. You can use it for stored procedures, triggers, and other procedural code that's callable from SQL. This language extension is supported by all current releases of PostgreSQL.

If you use [PLV8](#) and upgrade PostgreSQL to a new PLV8 version, you immediately take advantage of the new extension. Take the following steps to synchronize your catalog metadata with the new version of PLV8. These steps are optional, but we highly recommend that you complete them to avoid metadata mismatch warnings.

The upgrade process drops all your existing PLV8 functions. Thus, we recommend that you create a snapshot of your RDS for PostgreSQL DB instance before upgrading. For more information, see [Creating a DB snapshot \(p. 448\)](#).

To synchronize your catalog metadata with a new version of PLV8

1. Verify that you need to update. To do this, run the following command while connected to your instance.

```
SELECT * FROM pg_available_extensions WHERE name IN ('plv8','plls','plcoffee');
```

If your results contain values for an installed version that is a lower number than the default version, continue with this procedure to update your extensions. For example, the following result set indicates that you should update.

name	default_version	installed_version	comment
plls	2.1.0	1.5.3	PL/LiveScript (v8) trusted procedural language
plcoffee	2.1.0	1.5.3	PL/CoffeeScript (v8) trusted procedural language
plv8	2.1.0	1.5.3	PL/JavaScript (v8) trusted procedural language

2. Create a snapshot of your RDS for PostgreSQL DB instance if you haven't done so yet. You can continue with the following steps while the snapshot is being created.
3. Get a count of the number of PLV8 functions in your DB instance so you can validate that they are all in place after the upgrade. For example, the following SQL query returns the number of functions written in plv8, plcoffee, and plls.

```
SELECT proname, nspname, lanname
FROM pg_proc p, pg_language l, pg_namespace n
WHERE p.prolang = l.oid
AND n.oid = ppronamespace
AND lanname IN ('plv8','plcoffee','plls');
```

4. Use pg_dump to create a schema-only dump file. For example, create a file on your client machine in the /tmp directory.

```
./pg_dump -Fc --schema-only -U master postgres >/tmp/test.dmp
```

This example uses the following options:

- -Fc – Custom format

- --schema-only – Dump only the commands necessary to create schema (functions in this case)
- -U – The RDS master user name
- database – The database name for our DB instance

For more information on pg_dump, see [pg_dump](#) in the PostgreSQL documentation.

5. Extract the "CREATE FUNCTION" DDL statement that is present in the dump file. The following example uses the grep command to extract the DDL statement that creates the functions and save them to a file. You use this in subsequent steps to recreate the functions.

```
./pg_restore -l /tmp/test.dmp | grep FUNCTION > /tmp/function_list/
```

For more information on pg_restore, see [pg_restore](#) in the PostgreSQL documentation.

6. Drop the functions and extensions. The following example drops any PLV8 based objects. The cascade option ensures that any dependent are dropped.

```
DROP EXTENSION plv8 CASCADE;
```

If your PostgreSQL instance contains objects based on plcoffee or plls, repeat this step for those extensions.

7. Create the extensions. The following example creates the plv8, plcoffee, and plls extensions.

```
CREATE EXTENSION plv8;
CREATE EXTENSION plcoffee;
CREATE EXTENSION plls;
```

8. Create the functions using the dump file and "driver" file.

The following example recreates the functions that you extracted previously.

```
./pg_restore -U master -d postgres -Fc -L /tmp/function_list /tmp/test.dmp
```

9. Verify that all your functions have been recreated by using the following query.

```
SELECT * FROM pg_available_extensions WHERE name IN ('plv8','plls','plcoffee');
```

The PLV8 version 2 adds the following extra row to your result set:

proname	nspname	lanname
plv8_version	pg_catalog	plv8

Managing spatial data with the PostGIS extension

PostGIS is an extension to PostgreSQL for storing and managing spatial information. To learn more about PostGIS, see [PostGIS.net](#).

Starting with version 10.5, PostgreSQL supports the libprotobuf 1.3.0 library used by PostGIS for working with map box vector tile data.

Setting up the PostGIS extension requires `rds_superuser` privileges. We recommend that you create a user (role) to manage the PostGIS extension and your spatial data. The PostGIS extension and its related components add thousands of functions to PostgreSQL. Consider creating the PostGIS extension in its own schema if that makes sense for your use case. The following example shows how to install the extension in its own database, but this isn't required.

Topics

- [Step 1: Create a user \(role\) to manage the PostGIS extension \(p. 1980\)](#)
- [Step 2: Load the PostGIS extensions \(p. 1981\)](#)
- [Step 3: Transfer ownership of the extensions \(p. 1981\)](#)
- [Step 4: Transfer ownership of the PostGIS objects \(p. 1982\)](#)
- [Step 5: Test the extensions \(p. 1982\)](#)
- [Step 6: Upgrade the PostGIS extension \(p. 1983\)](#)
- [PostGIS extension versions \(p. 1983\)](#)
- [Upgrading PostGIS 2 to PostGIS 3 \(p. 1984\)](#)

Step 1: Create a user (role) to manage the PostGIS extension

First, connect to your RDS for PostgreSQL DB instance as a user that has `rds_superuser` privileges. If you kept the default name when you set up your instance, you connect as `postgres`.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres --password
```

Create a separate role (user) to administer the PostGIS extension.

```
postgres=> CREATE ROLE gis_admin LOGIN PASSWORD 'change_me';
CREATE ROLE
```

Grant this role `rds_superuser` privileges, to allow the role to install the extension.

```
postgres=> GRANT rds_superuser TO gis_admin;
GRANT
```

Create a database to use for your PostGIS artifacts. This step is optional. Or you can create a schema in your user database for the PostGIS extensions, but this also isn't required.

```
postgres=> CREATE DATABASE lab_gis;
CREATE DATABASE
```

Give the `gis_admin` all privileges on the `lab_gis` database.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_gis TO gis_admin;
```

GRANT

Exit the session and reconnect to your RDS for PostgreSQL DB instance as gis_admin.

```
postgres=> --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=gis_admin --password --dbname=lab_gis
Password for user gis_admin:...
lab_gis=>
```

Continue setting up the extension as detailed in the next steps.

Step 2: Load the PostGIS extensions

The PostGIS extension includes several related extensions that work together to provide geospatial functionality. Depending on your use case, you might not need all the extensions created in this step.

Use CREATE EXTENSION statements to load the PostGIS extensions.

```
CREATE EXTENSION postgis;
CREATE EXTENSION
CREATE EXTENSION postgis_raster;
CREATE EXTENSION
CREATE EXTENSION postgis_tiger_geocoder;
CREATE EXTENSION
CREATE EXTENSION postgis_topology;
CREATE EXTENSION
CREATE EXTENSION fuzzystrmatch;
CREATE EXTENSION
CREATE EXTENSION address_standardizer_data_us;
CREATE EXTENSION
```

You can verify the results by running the SQL query shown in the following example, which lists the extensions and their owners.

```
SELECT n.nspname AS "Name",
       pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
 WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
 ORDER BY 1;
List of schemas
   Name    |    Owner
-----+-----
 public   |    postgres
 tiger    |    rdsadmin
 tiger_data |    rdsadmin
 topology  |    rdsadmin
(4 rows)
```

Step 3: Transfer ownership of the extensions

Use the ALTER SCHEMA statements to transfer ownership of the schemas to the gis_admin role.

```
ALTER SCHEMA tiger OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA tiger_data OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA topology OWNER TO gis_admin;
ALTER SCHEMA
```

You can confirm the ownership change by running the following SQL query. Or you can use the \dn metacommand from the psql command line.

```
SELECT n.nspname AS "Name",
       pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
 WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
  ORDER BY 1;

List of schemas
 Name      | Owner
-----+-----
 public    | postgres
 tiger     | gis_admin
 tiger_data | gis_admin
 topology   | gis_admin
(4 rows)
```

Step 4: Transfer ownership of the PostGIS objects

Use the following function to transfer ownership of the PostGIS objects to the gis_admin role. Run the following statement from the psql prompt to create the function.

```
CREATE FUNCTION exec(text) returns text language plpgsql volatile AS $$ BEGIN EXECUTE $1;
  RETURN $1; END; $$;
CREATE FUNCTION
```

Next, run the following query to run the exec function that in turn runs the statements and alters the permissions.

```
SELECT exec('ALTER TABLE ' || quote_ident(s.nspname) || '.' || quote_ident(s.relname) || '
OWNER TO gis_admin;');
FROM (
  SELECT nspname, relname
  FROM pg_class c JOIN pg_namespace n ON (c.relnamespace = n.oid)
  WHERE nspname in ('tiger','topology') AND
    relkind IN ('r','S','v') ORDER BY relkind = 'S')
s;
```

Step 5: Test the extensions

To avoid needing to specify the schema name, add the tiger schema to your search path using the following command.

```
SET search_path=public,tiger;
SET
```

Test the tiger schema by using the following SELECT statement.

```
SELECT address, streetname, streettypeabbrev, zip
  FROM normalize_address('1 Devonshire Place, Boston, MA 02109') AS na;
address | streetname | streettypeabbrev | zip
-----+-----+-----+
1 | Devonshire | Pl | 02109
(1 row)
```

To learn more about this extension, see [Tiger Geocoder](#) in the PostGIS documentation.

Test access to the topology schema by using the following SELECT statement. This calls the `createtopology` function to register a new topology object (`my_new_topo`) with the specified spatial reference identifier (26986) and default tolerance (0.5). To learn more, see [CreateTopology](#) in the PostGIS documentation.

```
SELECT topology.createtopology('my_new_topo',26986,0.5);
createtopology
-----
      1
(1 row)
```

Step 6: Upgrade the PostGIS extension

Each new release of PostgreSQL supports one or more versions of the PostGIS extension compatible with that release. Upgrading the PostgreSQL engine to a new version doesn't automatically upgrade the PostGIS extension. Before upgrading the PostgreSQL engine, you typically upgrade PostGIS to the newest available version for the current PostgreSQL version. For details, see [PostGIS extension versions \(p. 1983\)](#).

After the PostgreSQL engine upgrade, you then upgrade the PostGIS extension again, to the version supported for the newly upgraded PostgreSQL engine version. For more information about upgrading the PostgreSQL engine, see [How to perform a major version upgrade \(p. 1843\)](#).

You can check for available PostGIS extension version updates on your RDS for PostgreSQL DB instance at any time. To do so, run the following command. This function is available with PostGIS 2.5.0 and higher versions.

```
SELECT postGIS_extensions_upgrade();
```

If your application doesn't support the latest PostGIS version, you can install an older version of PostGIS that's available in your major version as follows.

```
CREATE EXTENSION postgis VERSION "2.5.5";
```

If you want to upgrade to a specific PostGIS version from an older version, you can also use the following command.

```
ALTER EXTENSION postgis UPDATE TO "2.5.5";
```

Depending on the version that you're upgrading from, you might need to use this function again. The result of the first run of the function determines if an additional upgrade function is needed. For example, this is the case for upgrading from PostGIS 2 to PostGIS 3. For more information, see [Upgrading PostGIS 2 to PostGIS 3 \(p. 1984\)](#).

If you upgraded this extension to prepare for a major version upgrade of the PostgreSQL engine, you can continue with other preliminary tasks. For more information, see [How to perform a major version upgrade \(p. 1843\)](#).

PostGIS extension versions

We recommend that you install the versions of all extensions such as PostGIS as listed in [Extension versions for Amazon RDS for PostgreSQL](#) in the *Amazon RDS for PostgreSQL Release Notes*. To get a list of versions that are available in your release, use the following command.

```
SELECT * FROM pg_available_extension_versions WHERE name='postgis';
```

You can find version information in the following sections in the *Amazon RDS for PostgreSQL Release Notes*:

- [PostgreSQL version 14 extensions supported on Amazon RDS](#)
- [PostgreSQL version 13 extensions supported on Amazon RDS](#)
- [PostgreSQL version 12 extensions supported on Amazon RDS](#)
- [PostgreSQL version 11 extensions supported on Amazon RDS](#)
- [PostgreSQL version 10 extensions supported on Amazon RDS](#)
- [PostgreSQL version 9.6.x extensions supported on Amazon RDS](#)

Upgrading PostGIS 2 to PostGIS 3

Starting with version 3.0, the PostGIS raster functionality is now a separate extension, `postgis_raster`. This extension has its own installation and upgrade path. This removes dozens of functions, data types, and other artifacts required for raster image processing from the core `postgis` extension. That means that if your use case doesn't require raster processing, you don't need to install the `postgis_raster` extension.

In the following upgrade example, the first upgrade command extracts raster functionality into the `postgis_raster` extension. A second upgrade command is then required to upgrade `postgis_raster` to the new version.

To upgrade from PostGIS 2 to PostGIS 3

1. Identify the default version of PostGIS that's available to the PostgreSQL version on your RDS for PostgreSQL DB instance. To do so, run the following query.

```
SELECT * FROM pg_available_extensions
  WHERE default_version > installed_version;
   name | default_version | installed_version | comment
-----+-----+-----+
+-----+
 postgis | 3.1.4          | 2.3.7          | PostGIS geometry and geography spatial
 types and functions
(1 row)
```

2. Identify the versions of PostGIS installed in each database on your RDS for PostgreSQL DB instance. In other words, query each user database as follows.

```
SELECT
  e.extname AS "Name",
  e.extversion AS "Version",
  n.nspname AS "Schema",
  c.description AS "Description"
FROM
  pg_catalog.pg_extension e
  LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
  LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
    AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
  e.extname LIKE '%postgis%'
ORDER BY
  1;
   Name | Version | Schema | Description
-----+-----+-----+
+-----+
 postgis | 2.3.7 | public | PostGIS geometry, geography, and raster spatial types and
 functions
```

(1 row)

This mismatch between the default version (PostGIS 3.1.4) and the installed version (PostGIS 2.3.7) means that you need to upgrade the PostGIS extension.

```
ALTER EXTENSION postgis UPDATE;
ALTER EXTENSION
WARNING: unpackaging raster
WARNING: PostGIS Raster functionality has been unpackaged
```

- Run the following query to verify that the raster functionality is now in its own package.

```
SELECT
    probin,
    count(*)
FROM
    pg_proc
WHERE
    probin LIKE '%postgis%'
GROUP BY
    probin;
    probin      | count
-----+-----
$libdir/rtpostgis-2.3   | 107
$libdir/postgis-3       | 487
(2 rows)
```

The output shows that there's still a difference between versions. The PostGIS functions are version 3 (postgis-3), while the raster functions (rtpostgis) are version 2 (rtpostgis-2.3). To complete the upgrade, you run the upgrade command again, as follows.

```
postgres=> SELECT postgis_extensions_upgrade();
```

You can safely ignore the warning messages. Run the following query again to verify that the upgrade is complete. The upgrade is complete when PostGIS and all related extensions aren't marked as needing upgrade.

```
SELECT postgis_full_version();
```

- Use the following query to see the completed upgrade process and the separately packaged extensions, and verify that their versions match.

```
SELECT
    e.extname AS "Name",
    e.extversion AS "Version",
    n.nspname AS "Schema",
    c.description AS "Description"
FROM
    pg_catalog.pg_extension e
    LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
    LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
        AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
    e.extname LIKE '%postgis%'
ORDER BY
    1;
    Name      | Version | Schema | Description
-----+-----+-----+
+-----+
```

```
postgis      | 3.1.5   | public | PostGIS geometry, geography, and raster spatial
types and functions
postgis_raster | 3.1.5   | public | PostGIS raster types and functions
(2 rows)
```

The output shows that the PostGIS 2 extension was upgraded to PostGIS 3, and both `postgis` and the now separate `postgis_raster` extension are version 3.1.5.

After this upgrade completes, if you don't plan to use the raster functionality, you can drop the extension as follows.

```
DROP EXTENSION postgis_raster;
```

Working with the supported foreign data wrappers for Amazon RDS for PostgreSQL

A foreign data wrapper (FDW) is a specific type of extension that provides access to external data. For example, the `oracle_fdw` extension allows your RDS for PostgreSQL DB cluster to work with Oracle databases. As another example, by using the PostgreSQL native `postgres_fdw` extension you can access data stored in PostgreSQL DB instances external to your RDS for PostgreSQL DB instance.

Following, you can find information about several supported PostgreSQL foreign data wrappers.

Topics

- [Using the `log_fdw` extension to access the DB log using SQL \(p. 1987\)](#)
- [Using the `postgres_fdw` extension to access external data \(p. 1988\)](#)
- [Working with MySQL databases by using the `mysql_fdw` extension \(p. 1989\)](#)
- [Working with Oracle databases by using the `oracle_fdw` extension \(p. 1992\)](#)
- [Working with SQL Server databases by using the `tds_fdw` extension \(p. 1995\)](#)

Using the `log_fdw` extension to access the DB log using SQL

RDS for PostgreSQL supports the `log_fdw` extension, which you can use to access your database engine log using a SQL interface. The `log_fdw` extension provides two functions that make it easy to create foreign tables for database logs:

- `list_postgres_log_files` – Lists the files in the database log directory and the file size in bytes.
- `create_foreign_table_for_log_file(table_name text, server_name text, log_file_name text)` – Builds a foreign table for the specified file in the current database.

All functions created by `log_fdw` are owned by `rds_superuser`. Members of the `rds_superuser` role can grant access to these functions to other database users.

By default, the log files are generated by Amazon RDS in `stderr` (standard error) format, as specified in `log_destination` parameter. There are only two options for this parameter, `stderr` and `csvlog` (comma-separated values, CSV). If you add the `csvlog` option to the parameter, Amazon RDS generates both `stderr` and `csvlog` logs. This can affect the storage capacity on your instance, so you need to be aware of the other parameters that affect log handling. For more information, see [Setting the log destination \(`stderr`, `csvlog`\) \(p. 718\)](#).

One benefit of generating `csvlog` logs is that the `log_fdw` extension lets you build foreign tables with the data neatly split into several columns. To do this, your instance needs to be associated with a custom DB parameter group so that you can change the setting for `log_destination`. For more information about how to do so, see [Working with parameters on your RDS for PostgreSQL DB instance \(p. 1934\)](#).

The following example assumes that the `log_destination` parameter includes `cvslog`.

To use the `log_fdw` extension

1. Get the `log_fdw` extension.

```
postgres=> CREATE EXTENSION log_fdw;
CREATE EXTENSION
```

2. Create the log server as a foreign data wrapper.

```
postgres=> CREATE SERVER log_server FOREIGN DATA WRAPPER log_fdw;  
CREATE SERVER
```

3. Select all from a list of log files.

```
postgres=> SELECT * FROM list_postgres_log_files() ORDER BY 1;
```

A sample response is as follows.

file_name	file_size_bytes
postgresql.log.2016-08-09-22.csv	1111
postgresql.log.2016-08-09-23.csv	1172
postgresql.log.2016-08-10-00.csv	1744
postgresql.log.2016-08-10-01.csv	1102

(4 rows)

4. Create a table with a single 'log_entry' column for the selected file.

```
postgres=> SELECT create_foreign_table_for_log_file('my_postgres_error_log',  
'log_server', 'postgresql.log.2016-08-09-22.csv');
```

The response provides no detail other than that the table now exists.

```
-----  
(1 row)
```

5. Select a sample of the log file. The following code retrieves the log time and error message description.

```
postgres=> SELECT log_time, message FROM my_postgres_error_log ORDER BY 1;
```

A sample response is as follows.

log_time	message
Tue Aug 09 15:45:18.172 2016 PDT	ending log output to stderr
Tue Aug 09 15:45:18.175 2016 PDT	database system was interrupted; last known up at 2016-08-09 22:43:34 UTC
Tue Aug 09 15:45:18.223 2016 PDT	checkpoint record is at 0/90002E0
Tue Aug 09 15:45:18.223 2016 PDT	redo record is at 0/90002A8; shutdown FALSE
Tue Aug 09 15:45:18.223 2016 PDT	next transaction ID: 0/1879; next OID: 24578
Tue Aug 09 15:45:18.223 2016 PDT	next MultiXactId: 1; next MultiXactOffset: 0
Tue Aug 09 15:45:18.223 2016 PDT	oldest unfrozen transaction ID: 1822, in database 1

(7 rows)

Using the `postgres_fdw` extension to access external data

You can access data in a table on a remote database server with the `postgres_fdw` extension. If you set up a remote connection from your PostgreSQL DB instance, access is also available to your read replica.

To use `postgres_fdw` to access a remote database server

1. Install the `postgres_fdw` extension.

```
CREATE EXTENSION postgres_fdw;
```

2. Create a foreign data server using `CREATE SERVER`.

```
CREATE SERVER foreign_server
FOREIGN DATA WRAPPER postgres_fdw
OPTIONS (host 'xxx.xx.xxx.xx', port '5432', dbname 'foreign_db');
```

3. Create a user mapping to identify the role to be used on the remote server.

```
CREATE USER MAPPING FOR local_user
SERVER foreign_server
OPTIONS (user 'foreign_user', password 'password');
```

4. Create a table that maps to the table on the remote server.

```
CREATE FOREIGN TABLE foreign_table (
    id integer NOT NULL,
    data text)
SERVER foreign_server
OPTIONS (schema_name 'some_schema', table_name 'some_table');
```

Working with MySQL databases by using the `mysql_fdw` extension

To access a MySQL-compatible database from your RDS for PostgreSQL DB instance, you can install and use the `mysql_fdw` extension. This foreign data wrapper lets you work with RDS for MySQL, Aurora MySQL, MariaDB, and other MySQL-compatible databases. The connection from RDS for PostgreSQL to the MySQL database is encrypted on a best-effort basis, depending on the client and server configurations. However, you can enforce encryption if you like. For more information, see [Using encryption in transit with the extension \(p. 1992\)](#).

The `mysql_fdw` extension is supported on Amazon RDS for PostgreSQL version 14.2, 13.6, and higher releases. It supports selects, inserts, updates, and deletes from an RDS for PostgreSQL DB to tables on a MySQL-compatible database instance.

Topics

- [Setting up your RDS for PostgreSQL DB to use the `mysql_fdw` extension \(p. 1989\)](#)
- [Example: Working with an RDS for MySQL database from RDS for PostgreSQL \(p. 1991\)](#)
- [Using encryption in transit with the extension \(p. 1992\)](#)

Setting up your RDS for PostgreSQL DB to use the `mysql_fdw` extension

Setting up the `mysql_fdw` extension on your RDS for PostgreSQL DB instance involves loading the extension in your DB instance and then creating the connection point to the MySQL DB instance. For that task, you need to have the following details about the MySQL DB instance:

- Hostname or endpoint. For an RDS for MySQL DB instance, you can find the endpoint by using the Console. Choose the Connectivity & security tab and look in the "Endpoint and port" section.
- Port number. The default port number for MySQL is 3306.
- Name of the database. The DB identifier.

You also need to provide access on the security group or the access control list (ACL) for the MySQL port, 3306. Both the RDS for PostgreSQL DB instance and the RDS for MySQL DB instance need access to port 3306. If access isn't configured correctly, when you try to connect to MySQL-compatible table you see an error message similar to the following:

```
ERROR: failed to connect to MySQL: Can't connect to MySQL server on 'hostname.aws-region.rds.amazonaws.com:3306' (110)
```

In the following procedure, you (as the `rds_superuser` account) create the foreign server. You then grant access to the foreign server to specific users. These users then create their own mappings to the appropriate MySQL user accounts to work with the MySQL DB instance.

To use `mysql_fdw` to access a MySQL database server

1. Connect to your PostgreSQL DB instance using an account that has the `rds_superuser` role. If you accepted the defaults when you created your RDS for PostgreSQL DB instance, the user name is `postgres`, and you can connect using the `psql` command line tool as follows:

```
psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --  
username=postgres --password
```

2. Install the `mysql_fdw` extension as follows:

```
postgres=> CREATE EXTENSION mysql_fdw;  
CREATE EXTENSION
```

After the extension is installed on your RDS for PostgreSQL DB instance, you set up the foreign server that provides the connection to a MySQL database.

To create the foreign server

Perform these tasks on the RDS for PostgreSQL DB instance. The steps assume that you're connected as a user with `rds_superuser` privileges, such as `postgres`.

1. Create a foreign server in the RDS for PostgreSQL DB instance:

```
postgres=> CREATE SERVER mysql-db FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'db-name.111122223333.aws-region.rds.amazonaws.com', port '3306');  
CREATE SERVER
```

2. Grant the appropriate users access to the foreign server. These should be non-administrator users, that is, users without the `rds_superuser` role.

```
postgres=> GRANT USAGE ON FOREIGN SERVER mysql-db to user1;  
GRANT
```

PostgreSQL users create and manage their own connections to the MySQL database through the foreign server.

Example: Working with an RDS for MySQL database from RDS for PostgreSQL

Suppose that you have a simple table on an RDS for MySQL DB instance. Your RDS for PostgreSQL users want to query (SELECT), INSERT, UPDATE, and DELETE items on that table. Assume that the `mysql_fdw` extension was created on your RDS for PostgreSQL DB instance, as detailed in the preceding procedure. After you connect to the RDS for PostgreSQL DB instance as a user that has `rds_superuser` privileges, you can proceed with the following steps.

1. On the RDS for PostgreSQL DB instance, create a foreign server:

```
test=> CREATE SERVER mysqldb FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'your-DB.aws-region.rds.amazonaws.com', port '3306');  
CREATE SERVER
```

2. Grant usage to a user who doesn't have `rds_superuser` permissions, for example, `user1`:

```
test=> GRANT USAGE ON FOREIGN SERVER mysqldb TO user1;  
GRANT
```

3. Connect as `user1`, and then create a mapping to the MySQL user:

```
test=> CREATE USER MAPPING FOR user1 SERVER mysqldb OPTIONS (username 'myuser',  
password 'mypassword');  
CREATE USER MAPPING
```

4. Create a foreign table linked to the MySQL table:

```
test=> CREATE FOREIGN TABLE mytab (a int, b text) SERVER mysqldb OPTIONS (dbname  
'test', table_name '');  
CREATE FOREIGN TABLE
```

5. Run a simple query against the foreign table:

```
test=> SELECT * FROM mytab;  
a | b  
---+----  
1 | apple  
(1 row)
```

6. You can add, change, and remove data from the MySQL table. For example:

```
test=> INSERT INTO mytab values (2, 'mango');  
INSERT 0 1
```

Run the SELECT query again to see the results:

```
test=> SELECT * FROM mytab ORDER BY 1;  
a | b  
---+----  
1 | apple  
2 | mango  
(2 rows)
```

Using encryption in transit with the extension

The connection to MySQL from RDS for PostgreSQL uses encryption in transit (TLS/SSL) by default. However, the connection falls back to non-encrypted when the client and server configuration differ. You can enforce encryption for all outgoing connections by specifying the REQUIRE SSL option on the RDS for MySQL user accounts. This same approach also works for MariaDB and Aurora MySQL user accounts.

For MySQL user accounts configured to REQUIRE SSL, the connection attempt fails if a secure connection can't be established.

To enforce encryption for existing MySQL database user accounts, you can use the ALTER USER command. The syntax varies, depending on the MySQL version, as shown in the following table. For more information, see [ALTER USER](#) in *MySQL Reference Manual*.

MySQL 5.7, MySQL 8	MySQL 5.6
ALTER USER ' <i>user</i> '@'%' REQUIRE SSL;	GRANT USAGE ON *.* to ' <i>user</i> '@'%' REQUIRE SSL;

For more information about the mysql_fdw extension, see the [mysql_fdw](#) documentation.

Working with Oracle databases by using the oracle_fdw extension

To access an Oracle database from your RDS for PostgreSQL DB instance you can install and use the oracle_fdw extension. This extension is a foreign data wrapper for Oracle databases. To learn more about this extension, see the [oracle_fdw](#) documentation.

The oracle_fdw extension is supported on RDS for PostgreSQL 12.7, 13.3, and higher versions.

Topics

- [Turning on the oracle_fdw extension \(p. 1992\)](#)
- [Example: Using a foreign server linked to an Amazon RDS for Oracle database \(p. 1992\)](#)
- [Working with encryption in transit \(p. 1993\)](#)
- [Understanding the pg_user_mappings view and permissions \(p. 1993\)](#)

Turning on the oracle_fdw extension

To use the oracle_fdw extension, perform the following procedure.

To turn on the oracle_fdw extension

- Run the following command using an account that has rds_superuser permissions.

```
CREATE EXTENSION oracle_fdw;
```

Example: Using a foreign server linked to an Amazon RDS for Oracle database

The following example shows the use of a foreign server linked to an Amazon RDS for Oracle database.

To create a foreign server linked to an RDS for Oracle database

1. Note the following on the RDS for Oracle DB instance:

- Endpoint
- Port
- Database name

2. Create a foreign server.

```
test=> CREATE SERVER oradb FOREIGN DATA WRAPPER oracle_fdw OPTIONS (dbserver
'//endpoint:port/DB_name');
CREATE SERVER
```

3. Grant usage to a user who doesn't have rds_superuser privileges, for example user1.

```
test=> GRANT USAGE ON FOREIGN SERVER oradb TO user1;
GRANT
```

4. Connect as user1, and create a mapping to an Oracle user.

```
test=> CREATE USER MAPPING FOR user1 SERVER oradb OPTIONS (user 'oracleuser', password
'mypassword');
CREATE USER MAPPING
```

5. Create a foreign table linked to an Oracle table.

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER oradb OPTIONS (table 'MYTABLE');
CREATE FOREIGN TABLE
```

6. Query the foreign table.

```
test=> SELECT * FROM mytab;
a
---
1
(1 row)
```

If the query reports the following error, check your security group and access control list (ACL) to make sure that both instances can communicate.

```
ERROR: connection for foreign table "mytab" cannot be established
DETAIL: ORA-12170: TNS:Connect timeout occurred
```

Working with encryption in transit

PostgreSQL-to-Oracle encryption in transit is based on a combination of client and server configuration parameters. For an example using Oracle 21c, see [About the Values for Negotiating Encryption and Integrity](#) in the Oracle documentation. The client used for oracle_fdw on Amazon RDS is configured with ACCEPTED, meaning that the encryption depends on the Oracle database server configuration.

If your database is on RDS for Oracle, see [Oracle native network encryption](#) to configure the encryption.

Understanding the pg_user_mappings view and permissions

The PostgreSQL catalog pg_user_mapping stores the mapping from an RDS for PostgreSQL user to the user on a foreign data (remote) server. Access to the catalog is restricted, but you use the

pg_user_mappings view to see the mappings. In the following, you can find an example that shows how permissions apply with an example Oracle database, but this information applies more generally to any foreign data wrapper.

In the following output, you can find roles and permissions mapped to three different example users. Users rdssu1 and rdssu2 are members of the rds_superuser role, and user1 isn't. The example uses the psql metacommand \du to list existing roles.

```
test=> \du
          Role name | Member of | Attributes | List of roles |
-----+-----+-----+
+-----+-----+-----+
rdssu1 | {rds_superuser} |           |           |
rdssu2 | {rds_superuser} |           |           |
user1  |                   |           | {}
```

All users, including users that have rds_superuser privileges, are allowed to view their own user mappings (umoptions) in the pg_user_mappings table. As shown in the following example, when rdssu1 tries to obtain all user mappings, an error is raised even though rdssu1rds_superuser privileges:

```
test=> SELECT * FROM pg_user_mapping;
ERROR: permission denied for table pg_user_mapping
```

Following are some examples.

```
test=> SET SESSION AUTHORIZATION rdssu1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid | srvid | srvname | umuser | username | umoptions
-----+-----+-----+-----+-----+
 16414 | 16411 | oradb | 16412 | user1 | {user=oracleuser,password=mypwd}
 16423 | 16411 | oradb | 16421 | rdssu1 | {user=oracleuser,password=mypwd}
 16424 | 16411 | oradb | 16422 | rdssu2 | {user=oracleuser,password=mypwd}
(3 rows)

test=> SET SESSION AUTHORIZATION rdssu2;
SET
test=> SELECT * FROM pg_user_mappings;
 umid | srvid | srvname | umuser | username | umoptions
-----+-----+-----+-----+-----+
 16414 | 16411 | oradb | 16412 | user1 | {user=oracleuser,password=mypwd}
 16423 | 16411 | oradb | 16421 | rdssu1 | {user=oracleuser,password=mypwd}
 16424 | 16411 | oradb | 16422 | rdssu2 | {user=oracleuser,password=mypwd}
(3 rows)

test=> SET SESSION AUTHORIZATION user1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid | srvid | srvname | umuser | username | umoptions
-----+-----+-----+-----+-----+
 16414 | 16411 | oradb | 16412 | user1 | {user=oracleuser,password=mypwd}
 16423 | 16411 | oradb | 16421 | rdssu1 | {user=oracleuser,password=mypwd}
 16424 | 16411 | oradb | 16422 | rdssu2 | {user=oracleuser,password=mypwd}
(3 rows)
```

Because of implementation differences between `information_schema._pg_user_mappings` and `pg_catalog.pg_user_mappings`, a manually created `rds_superuser` requires additional permissions to view passwords in `pg_catalog.pg_user_mappings`.

No additional permissions are required for an `rds_superuser` to view passwords in `information_schema._pg_user_mappings`.

Users who don't have the `rds_superuser` role can view passwords in `pg_user_mappings` only under the following conditions:

- The current user is the user being mapped and owns the server or holds the USAGE privilege on it.
- The current user is the server owner and the mapping is for PUBLIC.

Working with SQL Server databases by using the tds_fdw extension

You can use the PostgreSQL `tds_fdw` extension to access databases that support the tabular data stream (TDS) protocol, such as Sybase and Microsoft SQL Server databases. This foreign data wrapper lets you connect from your RDS for PostgreSQL DB instance to databases that use the TDS protocol, including Amazon RDS for Microsoft SQL Server. For more information, see [tds-fdw/tds_fdw](#) documentation on GitHub.

The `tds_fdw` extension is supported on Amazon RDS for PostgreSQL version 14.2, 13.6, and higher releases.

Setting up your RDS for PostgreSQL DB to use the tds_fdw extension

In the following procedures, you can find an example of setting up and using the `tds_fdw` with an RDS for PostgreSQL DB instance. Before you can connect to a SQL Server database using `tds_fdw`, you need to get the following details for the instance:

- Hostname or endpoint. For an RDS for SQL Server DB instance, you can find the endpoint by using the Console. Choose the Connectivity & security tab and look in the "Endpoint and port" section.
- Port number. The default port number for Microsoft SQL Server is 1433.
- Name of the database. The DB identifier.

You also need to provide access on the security group or the access control list (ACL) for the SQL Server port, 1433. Both the RDS for PostgreSQL DB instance and the RDS for SQL Server DB instance need access to port 1433. If access isn't configured correctly, when you try to query the Microsoft SQL Server you see the following error message:

```
ERROR: DB-Library error: DB #: 20009, DB Msg: Unable to connect:  
Adaptive Server is unavailable or does not exist (mssql2019.aws-region.rds.amazonaws.com),  
OS #: 0, OS Msg: Success, Level: 9
```

To use tds_fdw to connect to a SQL Server database

1. Connect to your PostgreSQL DB instance using an account that has the `rds_superuser` role:

```
psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --username=test  
--password
```

2. Install the tds_fdw extension:

```
test=> CREATE EXTENSION tds_fdw;  
CREATE EXTENSION
```

After the extension is installed on your RDS for PostgreSQL DB instance, you set up the foreign server.

To create the foreign server

Perform these tasks on the RDS for PostgreSQL DB instance using an account that has rds_superuser privileges.

1. Create a foreign server in the RDS for PostgreSQL DB instance:

```
test=> CREATE SERVER sqlserverdb FOREIGN DATA WRAPPER tds_fdw OPTIONS (servername  
'mssql2019.aws-region.rds.amazonaws.com', port '1433', database 'tds_fdw_testing');  
CREATE SERVER
```

2. Grant permissions to a user who doesn't have rds_superuser role privileges, for example, user1:

```
test=> GRANT USAGE ON FOREIGN SERVER sqlserverdb TO user1;
```

3. Connect as user1 and create a mapping to a SQL Server user:

```
test=> CREATE USER MAPPING FOR user1 SERVER sqlserverdb OPTIONS (username  
'sqlserveruser', password 'password');  
CREATE USER MAPPING
```

4. Create a foreign table linked to a SQL Server table:

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER sqlserverdb OPTIONS (table 'MYTABLE');  
CREATE FOREIGN TABLE
```

5. Query the foreign table:

```
test=> SELECT * FROM mytab;  
a  
---  
1  
(1 row)
```

Using encryption in transit for the connection

The connection from RDS for PostgreSQL to SQL Server uses encryption in transit (TLS/SSL) depending on the SQL Server database configuration. If the SQL Server isn't configured for encryption, the RDS for PostgreSQL client making the request to the SQL Server database falls back to unencrypted.

You can enforce encryption for the connection to RDS for SQL Server DB instances by setting the `rds.force_ssl` parameter. To learn how, see [Forcing connections to your DB instance to use SSL](#). For more information about SSL/TLS configuration for RDS for SQL Server, see [Using SSL with a Microsoft SQL Server DB instance](#).

Security in Amazon RDS

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS compliance programs](#). To learn about the compliance programs that apply to Amazon RDS, see [AWS services in scope by compliance program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your organization's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon RDS. The following topics show you how to configure Amazon RDS to meet your security and compliance objectives. You also learn how to use other AWS services that help you monitor and secure your Amazon RDS resources.

You can manage access to your Amazon RDS resources and your databases on a DB instance. The method you use to manage access depends on what type of task the user needs to perform with Amazon RDS:

- Run your DB instance in a virtual private cloud (VPC) based on the Amazon VPC service for the greatest possible network access control. For more information about creating a DB instance in a VPC, see [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#).
- Use AWS Identity and Access Management (IAM) policies to assign permissions that determine who is allowed to manage Amazon RDS resources. For example, you can use IAM to determine who is allowed to create, describe, modify, and delete DB instances, tag resources, or modify security groups.
- Use security groups to control what IP addresses or Amazon EC2 instances can connect to your databases on a DB instance. When you first create a DB instance, its firewall prevents any database access except through rules specified by an associated security group.
- Use Secure Socket Layer (SSL) or Transport Layer Security (TLS) connections with DB instances running the MySQL, MariaDB, PostgreSQL, Oracle, or Microsoft SQL Server database engines. For more information on using SSL/TLS with a DB instance, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).
- Use Amazon RDS encryption to secure your DB instances and snapshots at rest. Amazon RDS encryption uses the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your DB instance. For more information, see [Encrypting Amazon RDS resources \(p. 2000\)](#).
- Use network encryption and transparent data encryption with Oracle DB instances; for more information, see [Oracle native network encryption \(p. 1711\)](#) and [Oracle Transparent Data Encryption \(p. 1751\)](#)
- Use the security features of your DB engine to control who can log in to the databases on a DB instance. These features work just as if the database was on your local network.

Note

You have to configure security only for your use cases. You don't have to configure security access for processes that Amazon RDS manages. These include creating backups, replicating data between a primary DB instance and a read replica, and other processes.

For more information on managing access to Amazon RDS resources and your databases on a DB instance, see the following topics.

Topics

- [Database authentication with Amazon RDS \(p. 1998\)](#)
- [Data protection in Amazon RDS \(p. 1999\)](#)
- [Identity and access management for Amazon RDS \(p. 2016\)](#)
- [Logging and monitoring in Amazon RDS \(p. 2077\)](#)
- [Compliance validation for Amazon RDS \(p. 2079\)](#)
- [Resilience in Amazon RDS \(p. 2080\)](#)
- [Infrastructure security in Amazon RDS \(p. 2081\)](#)
- [Amazon RDS API and interface VPC endpoints \(AWS PrivateLink\) \(p. 2082\)](#)
- [Security best practices for Amazon RDS \(p. 2084\)](#)
- [Controlling access with security groups \(p. 2085\)](#)
- [Master user account privileges \(p. 2087\)](#)
- [Using service-linked roles for Amazon RDS \(p. 2089\)](#)
- [Amazon VPC VPCs and Amazon RDS \(p. 2103\)](#)

Database authentication with Amazon RDS

Amazon RDS supports several ways to authenticate database users.

Password, Kerberos, and IAM database authentication use different methods of authenticating to the database. Therefore, a specific user can log in to a database using only one authentication method.

For PostgreSQL, use only one of the following role settings for a user of a specific database:

- To use IAM database authentication, assign the `rds_iam` role to the user.
- To use Kerberos authentication, assign the `rds_ad` role to the user.
- To use password authentication, don't assign either the `rds_iam` or `rds_ad` roles to the user.

Don't assign both the `rds_iam` and `rds_ad` roles to a user of a PostgreSQL database either directly or indirectly by nested grant access. If the `rds_iam` role is added to the master user, IAM authentication takes precedence over password authentication so the master user has to log in as an IAM user.

Topics

- [Password authentication \(p. 1998\)](#)
- [IAM database authentication \(p. 1999\)](#)
- [Kerberos authentication \(p. 1999\)](#)

Password authentication

With *password authentication*, your database performs all administration of user accounts. You create users with SQL statements such as `CREATE USER`, with the appropriate clause required by the DB engine for specifying passwords. For example, in MySQL the statement is `CREATE USER name IDENTIFIED BY password`, while in PostgreSQL, the statement is `CREATE USER name WITH PASSWORD password`.

With password authentication, your database controls and authenticates user accounts. If a DB engine has strong password management features, they can enhance security. Database authentication might be easier to administer using password authentication when you have small user communities. Because

clear text passwords are generated in this case, integrating with AWS Secrets Manager can enhance security.

For information about using Secrets Manager with Amazon RDS, see [Creating a basic secret](#) and [Rotating secrets for supported Amazon RDS databases](#) in the *AWS Secrets Manager User Guide*. For information about programmatically retrieving your secrets in your custom applications, see [Retrieving the secret value](#) in the *AWS Secrets Manager User Guide*.

IAM database authentication

You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MySQL and PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB instance. Instead, you use an authentication token.

For more information about IAM database authentication, including information about availability for specific DB engines, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

Kerberos authentication

Amazon RDS supports external authentication of database users using Kerberos and Microsoft Active Directory. Kerberos is a network authentication protocol that uses tickets and symmetric-key cryptography to eliminate the need to transmit passwords over the network. Kerberos has been built into Active Directory and is designed to authenticate users to network resources, such as databases.

Amazon RDS support for Kerberos and Active Directory provides the benefits of single sign-on and centralized authentication of database users. You can keep your user credentials in Active Directory. Active Directory provides a centralized place for storing and managing credentials for multiple DB instances.

You can make it possible for your database users to authenticate against DB instances in two ways. They can use credentials stored either in AWS Directory Service for Microsoft Active Directory or in your on-premises Active Directory.

Microsoft SQL Server, MySQL, and PostgreSQL DB instances support one- and two-way forest trust relationships. Oracle DB instances support one- and two-way external and forest trust relationships. For more information, see [When to create a trust relationship](#) in the *AWS Directory Service Administration Guide*.

For information about Kerberos authentication with a specific DB engine, see the following:

- [Using Windows Authentication with an Amazon RDS for SQL Server DB instance \(p. 1143\)](#)
- [Using Kerberos authentication for MySQL \(p. 1333\)](#)
- [Configuring Kerberos authentication for Amazon RDS for Oracle \(p. 1501\)](#)
- [Using Kerberos authentication with Amazon RDS for PostgreSQL \(p. 1823\)](#)

Note

Currently, Kerberos authentication isn't supported for MariaDB DB instances.

Data protection in Amazon RDS

The AWS [shared responsibility model](#) applies to data protection in Amazon Relational Database Service. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the

AWS services that you use. For more information about data privacy, see the [Data Privacy FAQ](#). For information about data protection in Europe, see the [AWS Shared Responsibility Model and GDPR](#) blog post on the [AWS Security Blog](#).

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see [Federal Information Processing Standard \(FIPS\) 140-2](#).

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Amazon RDS or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Topics

- [Protecting data using encryption \(p. 2000\)](#)
- [Internetwork traffic privacy \(p. 2015\)](#)

Protecting data using encryption

You can enable encryption for database resources. You can also encrypt connections to DB instances.

Topics

- [Encrypting Amazon RDS resources \(p. 2000\)](#)
- [AWS KMS key management \(p. 2004\)](#)
- [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#)
- [Rotating your SSL/TLS certificate \(p. 2007\)](#)

Encrypting Amazon RDS resources

Amazon RDS can encrypt your Amazon RDS DB instances. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, read replicas, and snapshots.

Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt your data on the server that hosts your Amazon RDS DB instances. After your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. You don't need to modify your database client applications to use encryption.

Note

For encrypted and unencrypted DB instances, data that is in transit between the source and the read replicas is encrypted, even when replicating across AWS Regions.

Topics

- [Overview of encrypting Amazon RDS resources \(p. 2001\)](#)
- [Encrypting a DB instance \(p. 2001\)](#)
- [Determining whether encryption is turned on for a DB instance \(p. 2002\)](#)
- [Availability of Amazon RDS encryption \(p. 2003\)](#)
- [Limitations of Amazon RDS encrypted DB instances \(p. 2003\)](#)

Overview of encrypting Amazon RDS resources

Amazon RDS encrypted DB instances provide an additional layer of data protection by securing your data from unauthorized access to the underlying storage. You can use Amazon RDS encryption to increase data protection of your applications deployed in the cloud, and to fulfill compliance requirements for encryption at rest.

Amazon RDS also supports encrypting an Oracle or SQL Server DB instance with Transparent Data Encryption (TDE). TDE can be used with RDS encryption at rest, although using TDE and RDS encryption at rest simultaneously might slightly affect the performance of your database. You must manage different keys for each encryption method. For more information on TDE, see [Oracle Transparent Data Encryption \(p. 1751\)](#) or [Support for Transparent Data Encryption in SQL Server \(p. 1217\)](#).

For an Amazon RDS encrypted DB instance, all logs, backups, and snapshots are encrypted. Amazon RDS uses an AWS KMS key to encrypt these resources. For more information about KMS keys, see [AWS KMS keys](#) in the *AWS Key Management Service Developer Guide*. If you copy an encrypted snapshot, you can use a different KMS key to encrypt the target snapshot than the one that was used to encrypt the source snapshot.

A read replica of an Amazon RDS encrypted instance must be encrypted using the same KMS key as the primary DB instance when both are in the same AWS Region. If the primary DB instance and read replica are in different AWS Regions, you encrypt the read replica using the KMS key for that AWS Region.

You can use an AWS managed key, or you can create customer managed keys. To manage the customer managed keys used for encrypting and decrypting your Amazon RDS resources, you use the [AWS Key Management Service \(AWS KMS\)](#). AWS KMS combines secure, highly available hardware and software to provide a key management system scaled for the cloud. Using AWS KMS, you can create customer managed keys and define the policies that control how these customer managed keys can be used. AWS KMS supports CloudTrail, so you can audit KMS key usage to verify that customer managed keys are being used appropriately. You can use your customer managed keys with Amazon Aurora and supported AWS services such as Amazon S3, Amazon EBS, and Amazon Redshift. For a list of services that are integrated with AWS KMS, see [AWS Service Integration](#).

Encrypting a DB instance

To encrypt a new DB instance, choose **Enable encryption** on the Amazon RDS console. For information on creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

If you use the `create-db-instance` AWS CLI command to create an encrypted DB instance, set the `--storage-encrypted` parameter. If you use the `CreateDBInstance` API operation, set the `StorageEncrypted` parameter to true.

When you create an encrypted DB instance, you can choose a customer managed key or the AWS managed key for Amazon RDS to encrypt your DB instance. If you don't specify the key identifier for a customer managed key, Amazon RDS uses the AWS managed key for your new DB instance. Amazon RDS creates an AWS managed key for Amazon RDS for your AWS account. Your AWS account has a different AWS managed key for Amazon RDS for each AWS Region.

Once you have created an encrypted DB instance, you can't change the KMS key used by that DB instance. Therefore, be sure to determine your KMS key requirements before you create your encrypted DB instance.

If you use the AWS CLI `create-db-instance` command to create an encrypted DB instance with a customer managed key, set the `--kms-key-id` parameter to any key identifier for the KMS key. If you use the Amazon RDS API `CreateDBInstance` operation, set the `KmsKeyId` parameter to any key identifier for the KMS key. To use a customer managed key in a different AWS account, specify the key ARN or alias ARN.

Important

Amazon RDS can lose access to the KMS key for a DB instance. For example, RDS loses access when the KMS key isn't enabled, or when RDS access to a KMS key is revoked. In these cases, the encrypted DB instance goes into `inaccessible-encryption-credentials-recoverable` state. The DB instance remains in this state for seven days. When you start the DB instance during that time, it checks if the KMS key is active and recovers the DB instance if it is. Restart the DB instance using the AWS CLI command `start-db-instance`. Currently, you can't start a DB instance in this state using the AWS Management Console.

If the DB instance isn't recovered, then it goes into the terminal `inaccessible-encryption-credentials` state. In this case, you can only restore the DB instance from a backup. We strongly recommend that you always turn on backups for encrypted DB instances to guard against the loss of encrypted data in your databases.

Determining whether encryption is turned on for a DB instance

You can use the AWS Management Console, AWS CLI, or RDS API to determine whether encryption at rest is turned on for a DB instance.

Console

To determine whether encryption at rest is turned on for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the name of the DB instance that you want to check to view its details.
4. Choose the **Configuration** tab, and check the **Encryption** value under **Storage**.

It shows either **Enabled** or **Not enabled**.

The screenshot shows the AWS RDS console interface. At the top, there's a breadcrumb trail: RDS > Databases > postgres-database-1. Below that is the instance name "postgres-database-1". On the right, there are "Modify" and "Actions" buttons. Under the "Summary" section, there are four columns: DB identifier (postgres-database-1), CPU (4.92%), Status (Available), and Class (db.t3.small). Role (Primary) and Current activity (0.00 sessions) are also listed. The "Configuration" tab is currently selected. In the "Instance" section, there are four columns: Configuration (DB instance ID: postgres-database-1), Instance class (db.t3.small), Storage (Encryption: Enabled), and Performance Insights (Performance Insights enabled: Yes). The "Storage" row is highlighted with a red box.

AWS CLI

To determine whether encryption at rest is turned on for a DB instance by using the AWS CLI, call the [describe-db-instances](#) command with the following option:

- `--db-instance-identifier` – The name of the DB instance.

The following example uses a query to return either TRUE or FALSE regarding encryption at rest for the `mydb` DB instance.

Example

```
aws rds describe-db-instances --db-instance-identifier mydb --query "*[].{StorageEncrypted:StorageEncrypted}" --output text
```

RDS API

To determine whether encryption at rest is turned on for a DB instance by using the Amazon RDS API, call the [DescribeDBInstances](#) operation with the following parameter:

- `DBInstanceIdentifier` – The name of the DB instance.

Availability of Amazon RDS encryption

Amazon RDS encryption is currently available for all database engines and storage types.

Amazon RDS encryption is available for most DB instance classes. The following table lists DB instance classes that *do not support* Amazon RDS encryption:

Instance type	Instance class
General purpose (M1)	db.m1.small
	db.m1.medium
	db.m1.large
	db.m1.xlarge
Memory optimized (M2)	db.m2.xlarge
	db.m2.2xlarge
	db.m2.4xlarge
Burstable (T2)	db.t2.micro

Note

Encryption at rest is not available for DB instances running SQL Server Express Edition.

Limitations of Amazon RDS encrypted DB instances

The following limitations exist for Amazon RDS encrypted DB instances:

- You can only encrypt an Amazon RDS DB instance when you create it, not after the DB instance is created.

However, because you can encrypt a copy of an unencrypted snapshot, you can effectively add encryption to an unencrypted DB instance. That is, you can create a snapshot of your DB instance, and then create an encrypted copy of that snapshot. You can then restore a DB instance from the encrypted snapshot, and thus you have an encrypted copy of your original DB instance. For more information, see [Copying a DB snapshot \(p. 458\)](#).

- You can't turn off encryption on an encrypted DB instance.
- You can't create an encrypted snapshot of an unencrypted DB instance.
- A snapshot of an encrypted DB instance must be encrypted using the same KMS key as the DB instance.
- You can't have an encrypted read replica of an unencrypted DB instance or an unencrypted read replica of an encrypted DB instance.
- Encrypted read replicas must be encrypted with the same KMS key as the source DB instance when both are in the same AWS Region.
- You can't restore an unencrypted backup or snapshot to an encrypted DB instance.
- To copy an encrypted snapshot from one AWS Region to another, you must specify the KMS key in the destination AWS Region. This is because KMS keys are specific to the AWS Region that they are created in.

The source snapshot remains encrypted throughout the copy process. Amazon RDS uses envelope encryption to protect data during the copy process. For more information about envelope encryption, see [Envelope encryption](#) in the [AWS Key Management Service Developer Guide](#).

- You can't unencrypt an encrypted DB instance. However, you can export data from an encrypted DB instance and import the data into an unencrypted DB instance.

AWS KMS key management

Amazon RDS automatically integrates with AWS Key Management Service (AWS KMS) for key management. Amazon RDS uses envelope encryption. For more information about envelope encryption, see [Envelope encryption](#) in the [AWS Key Management Service Developer Guide](#).

An *AWS KMS key* is a logical representation of a key. The KMS key includes metadata, such as the key ID, creation date, description, and key state. The KMS key also contains the key material used to encrypt and decrypt data. For more information about KMS keys, see [AWS KMS keys](#) in the [AWS Key Management Service Developer Guide](#).

You can manage KMS keys used for Amazon RDS encrypted DB instances using the [AWS Key Management Service \(AWS KMS\)](#) in the [AWS KMS console](#), the AWS CLI, or the AWS KMS API. If you want full control over a KMS key, then you must create a customer managed key. For more information about customer managed keys, see [Customer managed keys](#) in the [AWS Key Management Service Developer Guide](#).

AWS managed keys are KMS keys in your account that are created, managed, and used on your behalf by an AWS service that is integrated with AWS KMS. You can't delete, edit, or rotate AWS managed keys. For more information about AWS managed keys, see [AWS managed keys](#) in the [AWS Key Management Service Developer Guide](#).

You can't share a snapshot that has been encrypted using the AWS managed key of the AWS account that shared the snapshot.

You can view audit logs of every action taken with an AWS managed or customer managed key by using [AWS CloudTrail](#).

Important

If you turn off or revoke permissions to a KMS key used by an RDS database, RDS puts your database into a terminal state when access to the KMS key is required. This change could be

immediate, or deferred, depending on the use case that required access to the KMS key. In this state, the DB instance is no longer available, and the current state of the database can't be recovered. To restore the DB instance, you must re-enable access to the KMS key for RDS, and then restore the DB instance from the latest available backup.

Authorizing use of a customer managed key

When RDS uses a customer managed key in cryptographic operations, it acts on behalf of the user who is creating or changing the RDS resource.

To create an RDS resource using a customer managed key, a user must have permissions to call the following operations on the customer managed key:

- `kms:CreateGrant`
- `kms:DescribeKey`

You can specify these required permissions in a key policy, or in an IAM policy if the key policy allows it.

You can make the IAM policy stricter in various ways. For example, to allow the customer managed key to be used only for requests that originate in RDS, you can use the `kms:ViaService condition key` with the `rds.<region>.amazonaws.com` value.

You can also use the keys or values in the `encryption context` as a condition for using the customer managed key for cryptographic operations.

For more information, see [Allowing users in other accounts to use a KMS key](#) in the *AWS Key Management Service Developer Guide*.

Using SSL/TLS to encrypt a connection to a DB instance

You can use Secure Socket Layer (SSL) or Transport Layer Security (TLS) from your application to encrypt a connection to a DB instance running MariaDB, Microsoft SQL Server, MySQL, Oracle, or PostgreSQL.

SSL/TLS connections provide one layer of security by encrypting data that moves between your client and a DB instance. Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon RDS DB instance. It does so by checking the server certificate that is automatically installed on all DB instances that you provision.

Each DB engine has its own process for implementing SSL/TLS. To learn how to implement SSL/TLS for your DB instance, use the link following that corresponds to your DB engine:

- [Using SSL/TLS with a MariaDB DB instance \(p. 992\)](#)
- [Using SSL with a Microsoft SQL Server DB instance \(p. 1135\)](#)
- [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#)
- [Using SSL with an RDS for Oracle DB instance \(p. 1498\)](#)
- [Using SSL with a PostgreSQL DB instance \(p. 1816\)](#)

Note

All certificates are only available for download using SSL/TLS connections.

To get a certificate bundle that contains both the intermediate and root certificates for all AWS Regions, download from <https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem>.

If your application is on Microsoft Windows and requires a PKCS7 file, you can download the PKCS7 certificate bundle. This bundle contains both the intermediate and root certificates at <https://truststore.pki.rds.amazonaws.com/global/global-bundle.p7b>.

Note

Amazon RDS Proxy uses certificates from the AWS Certificate Manager (ACM). If you are using RDS Proxy, you don't need to download Amazon RDS certificates or update applications that use RDS Proxy connections. For more information about using TLS/SSL with RDS Proxy, see [Using TLS/SSL with RDS Proxy \(p. 927\)](#).

Certificate bundles for AWS Regions

To get a certificate bundle that contains both the intermediate and root certificates for an AWS Region, download from the link for the AWS Region in the following table.

AWS Region	Certificate bundle (PEM)	Certificate bundle (PKCS7)
US East (N. Virginia)	us-east-1-bundle.pem	us-east-1-bundle.p7b
US East (Ohio)	us-east-2-bundle.pem	us-east-2-bundle.p7b
US West (N. California)	us-west-1-bundle.pem	us-west-1-bundle.p7b
US West (Oregon)	us-west-2-bundle.pem	us-west-2-bundle.p7b
Africa (Cape Town)	af-south-1-bundle.pem	af-south-1-bundle.p7b
Asia Pacific (Hong Kong)	ap-east-1-bundle.pem	ap-east-1-bundle.p7b
Asia Pacific (Jakarta)	ap-southeast-3-bundle.pem	ap-southeast-3-bundle.p7b
Asia Pacific (Mumbai)	ap-south-1-bundle.pem	ap-south-1-bundle.p7b
Asia Pacific (Osaka)	ap-northeast-3-bundle.pem	ap-northeast-3-bundle.p7b
Asia Pacific (Tokyo)	ap-northeast-1-bundle.pem	ap-northeast-1-bundle.p7b
Asia Pacific (Seoul)	ap-northeast-2-bundle.pem	ap-northeast-2-bundle.p7b
Asia Pacific (Singapore)	ap-southeast-1-bundle.pem	ap-southeast-1-bundle.p7b
Asia Pacific (Sydney)	ap-southeast-2-bundle.pem	ap-southeast-2-bundle.p7b
Canada (Central)	ca-central-1-bundle.pem	ca-central-1-bundle.p7b
Europe (Frankfurt)	eu-central-1-bundle.pem	eu-central-1-bundle.p7b
Europe (Ireland)	eu-west-1-bundle.pem	eu-west-1-bundle.p7b
Europe (London)	eu-west-2-bundle.pem	eu-west-2-bundle.p7b
Europe (Milan)	eu-south-1-bundle.pem	eu-south-1-bundle.p7b
Europe (Paris)	eu-west-3-bundle.pem	eu-west-3-bundle.p7b
Europe (Stockholm)	eu-north-1-bundle.pem	eu-north-1-bundle.p7b
Middle East (Bahrain)	me-south-1-bundle.pem	me-south-1-bundle.p7b
Middle East (UAE)	me-central-1-bundle.pem	me-central-1-bundle.p7b
South America (São Paulo)	sa-east-1-bundle.pem	sa-east-1-bundle.p7b

AWS GovCloud (US) certificates

To get a certificate bundle that contains both the intermediate and root certificates for the AWS GovCloud (US) Regions, download from <https://truststore.pki.us-gov-west-1.rds.amazonaws.com/global/global-bundle.pem>.

If your application is on Microsoft Windows and requires a PKCS7 file, you can download the PKCS7 certificate bundle. This bundle contains both the intermediate and root certificates at <https://truststore.pki.us-gov-west-1.rds.amazonaws.com/global/global-bundle.p7b>.

To get a certificate bundle that contains both the intermediate and root certificates for an AWS GovCloud (US) Region, download from the link for the AWS GovCloud (US) Region in the following table.

AWS GovCloud (US) Region	Certificate bundle (PEM)	Certificate bundle (PKCS7)
AWS GovCloud (US-East)	us-gov-east-1-bundle.pem	us-gov-east-1-bundle.p7b
AWS GovCloud (US-West)	us-gov-west-1-bundle.pem	us-gov-west-1-bundle.p7b

Rotating your SSL/TLS certificate

As of March 5, 2020, Amazon RDS CA-2015 certificates have expired. If you use or plan to use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) with certificate verification to connect to your RDS DB instances, you require Amazon RDS CA-2019 certificates, which are enabled by default for new DB instances. If you currently do not use SSL/TLS with certificate verification, you might still have expired CA-2015 certificates and must update them to CA-2019 certificates if you plan to use SSL/TLS with certificate verification to connect to your RDS databases.

Follow these instructions to complete your updates. Before you update your DB instances to use the new CA certificate, make sure that you update your clients or applications connecting to your RDS databases.

Amazon RDS provides new CA certificates as an AWS security best practice. For information about the new certificates and the supported AWS Regions, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

Note

Amazon RDS Proxy uses certificates from the AWS Certificate Manager (ACM). If you are using RDS Proxy, when you rotate your SSL/TLS certificate, you don't need to update applications that use RDS Proxy connections. For more information about using TLS/SSL with RDS Proxy, see [Using TLS/SSL with RDS Proxy \(p. 927\)](#).

Note

If you are using a Go version 1.15 application with a DB instance that was created or updated to the rds-ca-2019 certificate prior to July 28, 2020, you must update the certificate again. Run the `modify-db-instance` command shown in the AWS CLI section using `rds-ca-2019` as the CA certificate identifier. In this case, it isn't possible to update the certificate using the AWS Management Console. If you created your DB instance or updated its certificate after July 28, 2020, no action is required. For more information, see [Go GitHub issue #39568](#).

Topics

- [Updating your CA certificate by modifying your DB instance \(p. 2007\)](#)
- [Updating your CA certificate by applying DB instance maintenance \(p. 2010\)](#)
- [Sample script for importing certificates into your trust store \(p. 2014\)](#)

Updating your CA certificate by modifying your DB instance

Complete the following steps to update your CA certificate.

To update your CA certificate by modifying your DB instance

1. Download the new SSL/TLS certificate as described in [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).
2. Update your applications to use the new SSL/TLS certificate.

The methods for updating applications for new SSL/TLS certificates depend on your specific applications. Work with your application developers to update the SSL/TLS certificates for your applications.

For information about checking for SSL/TLS connections and updating applications for each DB engine, see the following topics:

- [Using new SSL/TLS certificates for MariaDB DB instances \(p. 994\)](#)
- [Updating applications to connect to Microsoft SQL Server DB instances using new SSL/TLS certificates \(p. 1091\)](#)
- [Using new SSL/TLS certificates for MySQL DB instances \(p. 1330\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1498\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1819\)](#)

For a sample script that updates a trust store for a Linux operating system, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

The certificate bundle contains certificates for both the old and new CA, so you can upgrade your application safely and maintain connectivity during the transition period. If you are using the AWS Database Migration Service to migrate a database to a DB instance, we recommend using the certificate bundle to ensure connectivity during the migration.

3. Modify the DB instance to change the CA from **rds-ca-2015** to **rds-ca-2019**.

Important

By default, this operation restarts your DB instance. If you don't want to restart your DB instance during this operation, you can use the `modify-db-instance` CLI command and specify the `--no-certificate-rotation-restart` option.

This option will not rotate the certificate until the next time the database restarts, either for planned or unplanned maintenance. This option is only recommended if you don't use SSL/TLS.

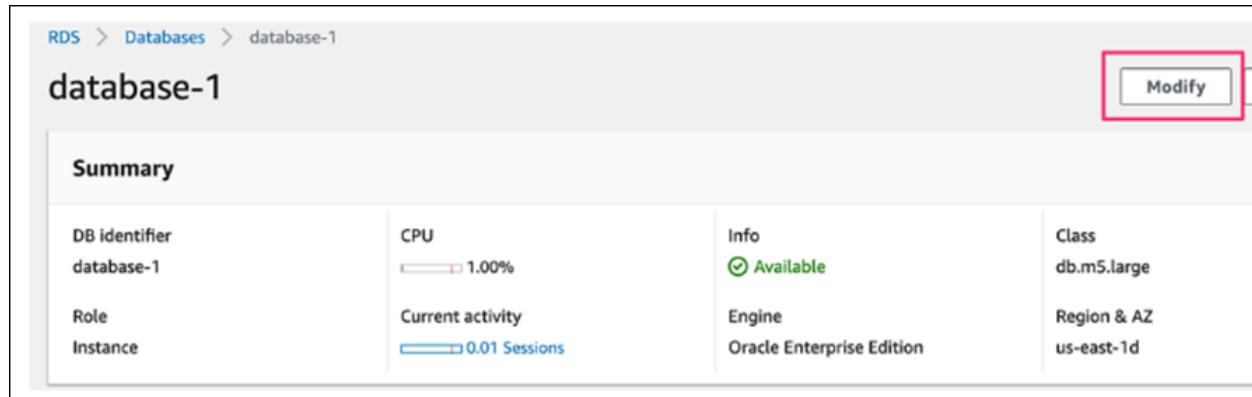
If you are experiencing connectivity issues after certificate expiry, use the `apply immediately` option by specifying **Apply immediately** in the console or by specifying the `--apply-immediately` option using the AWS CLI. By default, this operation is scheduled to run during your next maintenance window.

You can use the AWS Management Console or the AWS CLI to change the CA certificate from **rds-ca-2015** to **rds-ca-2019** for a DB instance.

Console

To change the CA from rds-ca-2015 to rds-ca-2019 for a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the DB instance that you want to modify.
3. Choose **Modify**.



The **Modify DB Instance** page appears.

4. In the **Connectivity** section, choose **rds-ca-2019**.

The screenshot shows the 'Certificate authority' section. A dropdown menu lists 'rds-ca-2019', 'rds-ca-2015', and 'rds-ca-2019' (which is highlighted). Below the dropdown, a note says: 'EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You can add more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.' There is also a radio button labeled 'No'.

5. Choose **Continue** and check the summary of modifications.
6. To apply the changes immediately, choose **Apply immediately**.

Important

Choosing this option restarts your database immediately.

7. On the confirmation page, review your changes. If they are correct, choose **Modify DB Instance** to save your changes.

Important

When you schedule this operation, make sure that you have updated your client-side trust store beforehand.

Or choose **Back** to edit your changes or **Cancel** to cancel your changes.

AWS CLI

To use the AWS CLI to change the CA from **rds-ca-2015** to **rds-ca-2019** for a DB instance, call the [modify-db-instance](#) command. Specify the DB instance identifier and the `--ca-certificate-identifier` option.

Important

When you schedule this operation, make sure that you have updated your client-side trust store beforehand.

Example

The following code modifies `mydbinstance` by setting the CA certificate to `rds-ca-2019`. The changes are applied during the next maintenance window by using `--no-apply-immediately`. Use `--apply-immediately` to apply the changes immediately.

Important

By default, this operation reboots your DB instance. If you don't want to reboot your DB instance during this operation, you can use the `modify-db-instance` CLI command and specify the `--no-certificate-rotation-restart` option.

This option will not rotate the certificate until the next time the database restarts, either for planned or unplanned maintenance. This option is only recommended if you do not use SSL/TLS.

Use `--apply-immediately` to apply the update immediately. By default, this operation is scheduled to run during your next maintenance window.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
  --db-instance-identifier mydbinstance \
  --ca-certificate-identifier rds-ca-2019 \
  --no-apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
  --db-instance-identifier mydbinstance ^
  --ca-certificate-identifier rds-ca-2019 ^
  --no-apply-immediately
```

Updating your CA certificate by applying DB instance maintenance

Complete the following steps to update your CA certificate by applying DB instance maintenance.

To update your CA certificate by applying DB instance maintenance

1. Download the new SSL/TLS certificate as described in [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).
2. Update your database applications to use the new SSL/TLS certificate.

The methods for updating applications for new SSL/TLS certificates depend on your specific applications. Work with your application developers to update the SSL/TLS certificates for your applications.

For information about checking for SSL/TLS connections and updating applications for each DB engine, see the following topics:

- [Using new SSL/TLS certificates for MariaDB DB instances \(p. 994\)](#)
- [Updating applications to connect to Microsoft SQL Server DB instances using new SSL/TLS certificates \(p. 1091\)](#)
- [Using new SSL/TLS certificates for MySQL DB instances \(p. 1330\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1498\)](#)
- [Updating applications to use new SSL/TLS certificates \(p. 1819\)](#)

For a sample script that updates a trust store for a Linux operating system, see [Sample script for importing certificates into your trust store \(p. 2014\)](#).

Note

The certificate bundle contains certificates for both the old and new CA, so you can upgrade your application safely and maintain connectivity during the transition period.

3. Apply DB instance maintenance to change the CA from **rds-ca-2015** to **rds-ca-2019**.

Important

You can choose to apply the change immediately. By default, this operation is scheduled to run during your next maintenance window.

You can use the AWS Management Console to apply DB instance maintenance to change the CA certificate from **rds-ca-2015** to **rds-ca-2019** for multiple DB instances.

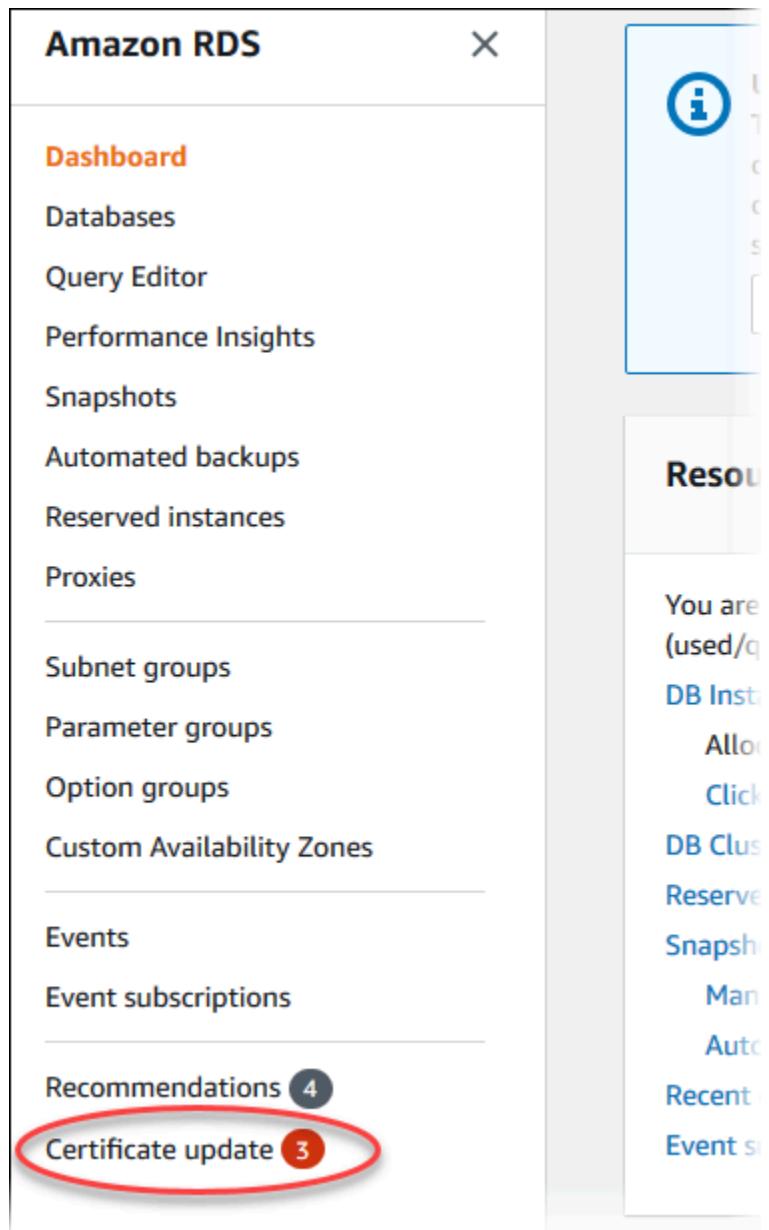
[Updating your CA certificate by applying maintenance to multiple DB instances](#)

Use the AWS Management Console to change the CA certificate for multiple DB instances.

To change the CA from rds-ca-2015 to rds-ca-2019 for multiple DB instances

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.

In the navigation pane, there is a **Certificate update** option that shows the total number of affected DB instances.



Choose **Certificate update** in the navigation pane.

The **Update your Amazon RDS SSL/TLS certificates** page appears.

DB identifier	DB cluster identifier	Status	Apply date
mydbinstancecf	-	Requires Update	-
mydbinstancecf2	-	Requires Update	-
oracledb	-	Requires Update	-

Note

This page only shows the DB instances for the current AWS Region. If you have DB instances in more than one AWS Region, check this page in each AWS Region to see all DB instances with old SSL/TLS certificates.

3. Choose the DB instance you want to update.

You can schedule the certificate rotation for your next maintenance window by choosing **Update at the next maintenance window**. Apply the rotation immediately by choosing **Update now**.

Important

When your CA certificate is rotated, the operation restarts your DB instance.

If you experience connectivity issues after certificate expiry, use the **Update now** option.

4. If you choose **Update at the next maintenance window** or **Update now**, you are prompted to confirm the CA certificate rotation.

Important

Before scheduling the CA certificate rotation on your database, update any client applications that use SSL/TLS and the server certificate to connect. These updates are specific to your DB engine. To determine whether your applications use SSL/TLS and the server certificate to connect, see [Step 2: Update Your Database Applications to Use the New SSL/TLS Certificate \(p. 2010\)](#). After you have updated these client applications, you can confirm the CA certificate rotation.

Confirm rotation of CA certificate?

Before scheduling the CA certificate rotation, update client applications that connect to your database to use the new CA certificate. Not doing this will cause an interruption of connectivity between your applications and your database. [Get new CA certificates](#)

I understand that not doing so will break SSL/TLS connectivity to my database.

Cancel

Confirm

To continue, choose the check box, and then choose **Confirm**.

5. Repeat steps 3 and 4 for each DB instance that you want to update.

Sample script for importing certificates into your trust store

The following are sample shell scripts that import the certificate bundle into a trust store.

Each sample shell script uses keytool, which is part of the Java Development Kit (JDK). For information about installing the JDK, see [JDK Installation Guide](#).

Topics

- [Sample script for importing certificates on Linux \(p. 2014\)](#)
- [Sample script for importing certificates on macOS \(p. 2014\)](#)

Sample script for importing certificates on Linux

The following is a sample shell script that imports the certificate bundle into a trust store on a Linux operating system.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" > ${mydir}/
global-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /----END CERTIFICATE----/ {split_after=1}{print
> "rds-ca-" n ".pem"}' < ${mydir}/global-bundle.pem

for CERT in rds-ca-*; do
alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /Subject:/; s/.*(CN=|CN = )//; print')
echo "Importing $alias"
keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -keystore
${truststore} -noprompt
rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias | cut -d
" " -f3- | while read alias
do
expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -alias
"${alias}" | grep Valid | perl -ne 'if(/until: (.*)\n/) { print "$1\n"; }'`
echo " Certificate ${alias} expires in '$expiry'"
done
```

Sample script for importing certificates on macOS

The following is a sample shell script that imports the certificate bundle into a trust store on macOS.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
```

```
mkdir -p "${mydir}"
fi

truststore=${mydir}/rds-truststore.jks
storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem" > ${mydir}/
global-bundle.pem
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/global-bundle.pem rds-ca-
for CERT in rds-ca-*; do
    alias=$(openssl x509 -noout -text -in $CERT | perl -ne 'next unless /Subject:/; s/.*(CN=|
CN = )//; print')
    echo "Importing $alias"
    keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -keystore
${truststore} -noprompt
    rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias | cut -d
" " -f3- | while read alias
do
    expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -alias
"${alias}" | grep Valid | perl -ne 'if(/until: (.*)\n/) { print "$1\n"; }'`
    echo " Certificate ${alias} expires in '$expiry'"
done
```

Internetwork traffic privacy

Connections are protected both between Amazon RDS and on-premises applications and between Amazon RDS and other AWS resources within the same AWS Region.

Traffic between service and on-premises clients and applications

You have two connectivity options between your private network and AWS:

- An AWS Site-to-Site VPN connection. For more information, see [What is AWS Site-to-Site VPN?](#)
- An AWS Direct Connect connection. For more information, see [What is AWS Direct Connect?](#)

You get access to Amazon RDS through the network by using AWS-published API operations. Clients must support Transport Layer Security (TLS) 1.0. We recommend TLS 1.2. Clients must also support cipher suites with Perfect Forward Secrecy (PFS), such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Most modern systems such as Java 7 and later support these modes. Additionally, you must sign requests using an access key identifier and a secret access key that are associated with an IAM principal. Or you can use the [AWS security token service \(STS\)](#) to generate temporary security credentials to sign requests.

Identity and access management for Amazon RDS

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon RDS resources. IAM is an AWS service that you can use with no additional charge.

Topics

- [Audience \(p. 2016\)](#)
- [Authenticating with identities \(p. 2016\)](#)
- [Managing access using policies \(p. 2018\)](#)
- [How Amazon RDS works with IAM \(p. 2020\)](#)
- [Identity-based policy examples for Amazon RDS \(p. 2025\)](#)
- [AWS managed policies for Amazon RDS \(p. 2036\)](#)
- [Amazon RDS updates to AWS managed policies \(p. 2043\)](#)
- [Preventing cross-service confused deputy problems \(p. 2046\)](#)
- [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#)
- [Troubleshooting Amazon RDS identity and access \(p. 2075\)](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work you do in Amazon RDS.

Service user – If you use the Amazon RDS service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon RDS features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon RDS, see [Troubleshooting Amazon RDS identity and access \(p. 2075\)](#).

Service administrator – If you're in charge of Amazon RDS resources at your company, you probably have full access to Amazon RDS. It's your job to determine which Amazon RDS features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon RDS, see [How Amazon RDS works with IAM \(p. 2020\)](#).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon RDS. To view example Amazon RDS identity-based policies that you can use in IAM, see [Identity-based policy examples for Amazon RDS \(p. 2025\)](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see [The IAM console and sign-in page](#) in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication, or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the [AWS Management Console](#), use your password with your root user email or your IAM user name. You can access AWS programmatically using your root user or IAM user access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see [Signature Version 4 signing process](#) in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the *AWS account root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *AWS General Reference*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see [Managing access keys for IAM users](#) in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

You can authenticate to your DB instance using IAM database authentication.

IAM database authentication works with the following DB engines:

- RDS for MariaDB
- RDS for MySQL
- RDS for PostgreSQL

For more information about authenticating to your DB instance using IAM, see [IAM database authentication for MariaDB, MySQL, and PostgreSQL \(p. 2048\)](#).

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API

operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see [Permission sets](#) in the *AWS IAM Identity Center (successor to AWS Single Sign-On) User Guide*.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
 - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for Amazon RDS](#) in the *Service Authorization Reference*.
 - **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
 - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when an entity (root user, IAM user, or IAM role) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored

in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, role, or group. These policies control what actions that identity can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

For information about AWS managed policies that are specific to Amazon RDS, see [AWS managed policies for Amazon RDS \(p. 2036\)](#).

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

How Amazon RDS works with IAM

Before you use IAM to manage access to Amazon RDS, you should understand what IAM features are available to use with Amazon RDS.

IAM features you can use with Amazon RDS

IAM feature	Amazon RDS support
Identity-based policies (p. 2021)	Yes
Resource-based policies (p. 2021)	No
Policy actions (p. 2021)	Yes
Policy resources (p. 2022)	Yes
Policy condition keys (service-specific) (p. 2023)	Yes
ACLs (p. 2024)	No
Attribute-based access control (ABAC) (tags in policies) (p. 2024)	Yes
Temporary credentials (p. 2024)	Yes
Principal permissions (p. 2025)	Yes
Service roles (p. 2025)	Yes
Service-linked roles (p. 2025)	Yes

To get a high-level view of how Amazon RDS and other AWS services work with IAM, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Topics

- [Amazon RDS identity-based policies \(p. 2021\)](#)
- [Resource-based policies within Amazon RDS \(p. 2021\)](#)
- [Policy actions for Amazon RDS \(p. 2021\)](#)
- [Policy resources for Amazon RDS \(p. 2022\)](#)
- [Policy condition keys for Amazon RDS \(p. 2023\)](#)
- [Access control lists \(ACLs\) in Amazon RDS \(p. 2024\)](#)
- [Attribute-based access control \(ABAC\) in policies with Amazon RDS tags \(p. 2024\)](#)
- [Using temporary credentials with Amazon RDS \(p. 2024\)](#)
- [Cross-service principal permissions for Amazon RDS \(p. 2025\)](#)
- [Service roles for Amazon RDS \(p. 2025\)](#)
- [Service-linked roles for Amazon RDS \(p. 2025\)](#)

Amazon RDS identity-based policies

Supports identity-based policies	Yes
----------------------------------	-----

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see [IAM JSON policy elements reference](#) in the *IAM User Guide*.

Identity-based policy examples for Amazon RDS

To view examples of Amazon RDS identity-based policies, see [Identity-based policy examples for Amazon RDS \(p. 2025\)](#).

Resource-based policies within Amazon RDS

Supports resource-based policies	No
----------------------------------	----

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are *IAM role trust policies* and *Amazon S3 bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Policy actions for Amazon RDS

Supports policy actions	Yes
-------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also

some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon RDS use the following prefix before the action: `rds:`. For example, to grant someone permission to describe DB instances with the Amazon RDS `DescribeDBInstances` API operation, you include the `rds:DescribeDBInstances` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Amazon RDS defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows.

```
"Action": [  
    "rds:action1",  
    "rds:action2"]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action.

```
"Action": "rds:Describe*"
```

To see a list of Amazon RDS actions, see [Actions Defined by Amazon RDS in the Service Authorization Reference](#).

Policy resources for Amazon RDS

Supports policy resources	Yes
---------------------------	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its [Amazon Resource Name \(ARN\)](#). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

The DB instance resource has the following Amazon Resource Name (ARN).

```
arn:${Partition}:rds:${Region}:${Account}:{ResourceType}/${Resource}
```

For more information about the format of ARNs, see [Amazon Resource Names \(ARNs\) and AWS service namespaces](#).

For example, to specify the dbtest DB instance in your statement, use the following ARN.

```
"Resource": "arn:aws:rds:us-west-2:123456789012:db:dbtest"
```

To specify all DB instances that belong to a specific account, use the wildcard (*).

```
"Resource": "arn:aws:rds:us-east-1:123456789012:db:/*"
```

Some RDS API operations, such as those for creating resources, can't be performed on a specific resource. In those cases, use the wildcard (*).

```
"Resource": "*"
```

Many Amazon RDS API operations involve multiple resources. For example, `CreateDBInstance` creates a DB instance. You can specify that an IAM user must use a specific security group and parameter group when creating a DB instance. To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [  
    "resource1",  
    "resource2"]
```

To see a list of Amazon RDS resource types and their ARNs, see [Resources Defined by Amazon RDS](#) in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see [Actions Defined by Amazon RDS](#).

Policy condition keys for Amazon RDS

Supports service-specific policy condition keys	Yes
---	-----

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition block`) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use [condition operators](#), such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical AND operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical OR operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see [IAM policy elements: variables and tags](#) in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

Amazon RDS defines its own set of condition keys and also supports using some global condition keys. To see all AWS global condition keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

All RDS API operations support the `aws:RequestedRegion` condition key.

To see a list of Amazon RDS condition keys, see [Condition Keys for Amazon RDS](#) in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see [Actions Defined by Amazon RDS](#).

Access control lists (ACLs) in Amazon RDS

Supports access control lists (ACLs)	No
--------------------------------------	----

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Attribute-based access control (ABAC) in policies with Amazon RDS tags

Supports attribute-based access control (ABAC) tags in policies	Yes
---	-----

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the [condition element](#) of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see [What is ABAC?](#) in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see [Use attribute-based access control \(ABAC\)](#) in the *IAM User Guide*.

For more information about tagging Amazon RDS resources, see [Specifying conditions: Using custom tags \(p. 2032\)](#). To view an example identity-based policy for limiting access to a resource based on the tags on that resource, see [Grant permission for actions on a resource with a specific tag with two different values \(p. 2030\)](#).

Using temporary credentials with Amazon RDS

Supports temporary credentials	Yes
--------------------------------	-----

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see [AWS services that work with IAM](#) in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see [Switching to a role \(console\)](#) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary

credentials instead of using long-term access keys. For more information, see [Temporary security credentials in IAM](#).

Cross-service principal permissions for Amazon RDS

Supports principal permissions	Yes
--------------------------------	-----

When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see [Actions, Resources, and Condition Keys for Amazon RDS](#) in the *Service Authorization Reference*.

Service roles for Amazon RDS

Supports service roles	Yes
------------------------	-----

A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.

Warning

Changing the permissions for a service role might break Amazon RDS functionality. Edit service roles only when Amazon RDS provides guidance to do so.

Service-linked roles for Amazon RDS

Supports service-linked roles	Yes
-------------------------------	-----

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about using Amazon RDS service-linked roles, see [Using service-linked roles for Amazon RDS \(p. 2089\)](#).

Identity-based policy examples for Amazon RDS

By default, IAM users and roles don't have permission to create or modify Amazon RDS resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see [Creating policies on the JSON tab](#) in the *IAM User Guide*.

Topics

- [Policy best practices \(p. 2026\)](#)
- [Using the Amazon RDS console \(p. 2026\)](#)
- [Allow users to view their own permissions \(p. 2027\)](#)

- Allow a user to create DB instances in an AWS account (p. 2027)
- Permissions required to use the console (p. 2029)
- Allow a user to perform any describe action on any RDS resource (p. 2029)
- Allow a user to create a DB instance that uses the specified DB parameter group and subnet group (p. 2029)
- Grant permission for actions on a resource with a specific tag with two different values (p. 2030)
- Prevent a user from deleting a DB instance (p. 2030)
- Deny all access to a resource (p. 2030)
- Example policies: Using condition keys (p. 2031)
- Specifying conditions: Using custom tags (p. 2032)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon RDS resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or root users in your account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

Using the Amazon RDS console

To access the Amazon RDS console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon RDS resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

To ensure that those entities can still use the Amazon RDS console, also attach the following AWS managed policy to the entities.

AmazonRDSReadOnlyAccess

For more information, see [Adding permissions to a user](#) in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "ViewOwnUserInfo",  
            "Effect": "Allow",  
            "Action": [  
                "iam:GetUserPolicy",  
                "iam>ListGroupsForUser",  
                "iam>ListAttachedUserPolicies",  
                "iam>ListUserPolicies",  
                "iam GetUser"  
            ],  
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]  
        },  
        {  
            "Sid": "NavigateInConsole",  
            "Effect": "Allow",  
            "Action": [  
                "iam:GetGroupPolicy",  
                "iam:GetPolicyVersion",  
                "iam GetPolicy",  
                "iam>ListAttachedGroupPolicies",  
                "iam>ListGroupPolicies",  
                "iam>ListPolicyVersions",  
                "iam>ListPolicies",  
                "iam>ListUsers"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Allow a user to create DB instances in an AWS account

The following is an example policy that allows the user with the ID 123456789012 to create DB instances for your AWS account. The policy requires that the name of the new DB instance begin with test. The new DB instance must also use the MySQL database engine and the db.t2.micro DB instance class. In addition, the new DB instance must use an option group and a DB parameter group that starts with default, and it must use the default subnet group.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Sid": "AllowCreateDBInstanceOnly",
        "Effect": "Allow",
        "Action": [
            "rds>CreateDBInstance"
        ],
        "Resource": [
            "arn:aws:rds:*:123456789012:db:test*",
            "arn:aws:rds:*:123456789012:og:default*",
            "arn:aws:rds:*:123456789012:pg:default*",
            "arn:aws:rds:*:123456789012:subgrp:default"
        ],
        "Condition": {
            "StringEquals": {
                "rds:DatabaseEngine": "mysql",
                "rds:DatabaseClass": "db.t2.micro"
            }
        }
    }
]
```

The policy includes a single statement that specifies the following permissions for the IAM user:

- The policy allows the IAM user to create a DB instance using the [CreateDBInstance](#) API operation (this also applies to the [create-db-instance](#) AWS CLI command and the AWS Management Console).
- The Resource element specifies that the user can perform actions on or with resources. You specify resources using an Amazon Resources Name (ARN). This ARN includes the name of the service that the resource belongs to (rds), the AWS Region (* indicates any region in this example), the user account number (123456789012 is the user ID in this example), and the type of resource. For more information about creating ARNs, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

The Resource element in the example specifies the following policy constraints on resources for the user:

- The DB instance identifier for the new DB instance must begin with test (for example, testCustomerData1, test-region2-data).
- The option group for the new DB instance must begin with default.
- The DB parameter group for the new DB instance must begin with default.
- The subnet group for the new DB instance must be the default subnet group.
- The Condition element specifies that the DB engine must be MySQL and the DB instance class must be db.t2.micro. The Condition element specifies the conditions when a policy should take effect. You can add additional permissions or restrictions by using the Condition element. For more information about specifying conditions, see [Policy condition keys for Amazon RDS \(p. 203\)](#). This example specifies the rds:DatabaseEngine and rds:DatabaseClass conditions. For information about the valid condition values for rds:DatabaseEngine, see the list under the Engine parameter in [CreateDBInstance](#). For information about the valid condition values for rds:DatabaseClass, see [Supported DB engines for DB instance classes \(p. 12\)](#).

The policy doesn't specify the Principal element because in an identity-based policy you don't specify the principal who gets the permission. When you attach policy to a user, the user is the implicit principal. When you attach a permission policy to an IAM role, the principal identified in the role's trust policy gets the permissions.

To see a list of Amazon RDS actions, see [Actions Defined by Amazon RDS in the Service Authorization Reference](#).

Permissions required to use the console

For a user to work with the console, that user must have a minimum set of permissions. These permissions allow the user to describe the Amazon RDS resources for their AWS account and to provide other related information, including Amazon EC2 security and network information.

If you create an IAM policy that is more restrictive than the minimum required permissions, the console doesn't function as intended for users with that IAM policy. To ensure that those users can still use the console, also attach the `AmazonRDSReadOnlyAccess` managed policy to the user, as described in [Managing access using policies \(p. 2018\)](#).

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the Amazon RDS API.

The following policy grants full access to all Amazon RDS resources for the root AWS account:

```
AmazonRDSFullAccess
```

Allow a user to perform any describe action on any RDS resource

The following permissions policy grants permissions to a user to run all of the actions that begin with `Describe`. These actions show information about an RDS resource, such as a DB instance. The wildcard character (*) in the `Resource` element indicates that the actions are allowed for all Amazon RDS resources owned by the account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRDSDescribe",
      "Effect": "Allow",
      "Action": "rds:Describe*",
      "Resource": "*"
    }
  ]
}
```

Allow a user to create a DB instance that uses the specified DB parameter group and subnet group

The following permissions policy grants permissions to allow a user to only create a DB instance that must use the `mydbpg` DB parameter group and the `mydbsubnetgroup` DB subnet group.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "rds>CreateDBInstance",
      "Resource": [
        "arn:aws:rds:*:pg:mydbpg",
        "arn:aws:rds:*:subgrp:mydbsubnetgroup"
      ]
    }
  ]
}
```

```
        ]
    }
}
```

Grant permission for actions on a resource with a specific tag with two different values

You can use conditions in your identity-based policy to control access to Amazon RDS resources based on tags. The following policy allows permission to perform the `ModifyDBInstance` and `CreateDBSnapshot` API operations on DB instances with either the stage tag set to `development` or `test`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDevTestCreate",
            "Effect": "Allow",
            "Action": [
                "rds:ModifyDBInstance",
                "rds:CreateDBSnapshot"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "rds:db-tag/stage": [
                        "development",
                        "test"
                    ]
                }
            }
        ]
    }
}
```

Prevent a user from deleting a DB instance

The following permissions policy grants permissions to prevent a user from deleting a specific DB instance. For example, you might want to deny the ability to delete your production DB instances to any user that is not an administrator.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyDelete1",
            "Effect": "Deny",
            "Action": "rds>DeleteDBInstance",
            "Resource": "arn:aws:rds:us-west-2:123456789012:db:my-mysql-instance"
        }
    ]
}
```

Deny all access to a resource

You can explicitly deny access to a resource. Deny policies take precedence over allow policies. The following policy explicitly denies a user the ability to manage a resource:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "rds:*",  
            "Resource": "arn:aws:rds:us-east-1:123456789012:db:mydb"  
        }  
    ]  
}
```

Example policies: Using condition keys

Following are examples of how you can use condition keys in Amazon RDS IAM permissions policies.

Example 1: Grant permission to create a DB instance that uses a specific DB engine and isn't MultiAZ

The following policy uses an RDS condition key and allows a user to create only DB instances that use the MySQL database engine and don't use MultiAZ. The Condition element indicates the requirement that the database engine is MySQL.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowMySQLCreate",  
            "Effect": "Allow",  
            "Action": "rds>CreateDBInstance",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "rds:DatabaseEngine": "mysql"  
                },  
                "Bool": {  
                    "rds:MultiAz": false  
                }  
            }  
        }  
    ]  
}
```

Example 2: Explicitly deny permission to create DB instances for certain DB instance classes and create DB instances that use Provisioned IOPS

The following policy explicitly denies permission to create DB instances that use the DB instance classes `r3.8xlarge` and `m4.10xlarge`, which are the largest and most expensive DB instance classes. This policy also prevents users from creating DB instances that use Provisioned IOPS, which incurs an additional cost.

Explicitly denying permission supersedes any other permissions granted. This ensures that identities do not accidentally get permission that you never want to grant.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DenyLargeCreate",  
            "Effect": "Deny",  
            "Action": "rds>CreateDBInstance",  
            "Resource": "arn:aws:rds:  
            "Condition": {  
                "StringNotEquals": {  
                    "rds:DBInstanceClass": "r3.8xlarge",  
                    "rds:DBInstanceClass": "m4.10xlarge",  
                    "rds:ProvisionedIOPS": "false"  
                }  
            }  
        }  
    ]  
}
```

```

    "Action": "rds>CreateDBInstance",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "rds:DatabaseClass": [
                "db.r3.8xlarge",
                "db.m4.10xlarge"
            ]
        }
    },
    {
        "Sid": "DenyPIOPSCreate",
        "Effect": "Deny",
        "Action": "rds>CreateDBInstance",
        "Resource": "*",
        "Condition": {
            "NumericNotEquals": {
                "rds:Piops": "0"
            }
        }
    }
]
}

```

Example 3: Limit the set of tag keys and values that can be used to tag a resource

The following policy uses an RDS condition key and allows the addition of a tag with the key `stage` to be added to a resource with the values `test`, `qa`, and `production`.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds>AddTagsToResource",
                "rds>RemoveTagsFromResource"
            ],
            "Resource": "*",
            "Condition": {
                "streq": {
                    "rds:req-tag/stage": [
                        "test",
                        "qa",
                        "production"
                    ]
                }
            }
        ]
    }
}

```

Specifying conditions: Using custom tags

Amazon RDS supports specifying conditions in an IAM policy using custom tags.

For example, suppose that you add a tag named `environment` to your DB instances with values such as `beta`, `staging`, `production`, and so on. If you do, you can create a policy that restricts certain users to DB instances based on the `environment` tag value.

Note

Custom tag identifiers are case-sensitive.

The following table lists the RDS tag identifiers that you can use in a Condition element.

RDS tag identifier	Applies to
db-tag	DB instances, including read replicas
snapshot-tag	DB snapshots
ri-tag	Reserved DB instances
og-tag	DB option groups
pg-tag	DB parameter groups
subgrp-tag	DB subnet groups
es-tag	Event subscriptions
cluster-tag	DB clusters
cluster-pg-tag	DB cluster parameter groups
cluster-snapshot-tag	DB cluster snapshots

The syntax for a custom tag condition is as follows:

```
"Condition": {"StringEquals": {"rds:rds-tag-identifier/tag-name": ["value"]}} }
```

For example, the following Condition element applies to DB instances with a tag named environment and a tag value of production.

```
"Condition": {"StringEquals": {"rds:db-tag/environment": ["production"]}} }
```

For information about creating tags, see [Tagging Amazon RDS resources \(p. 392\)](#).

Important

If you manage access to your RDS resources using tagging, we recommend that you secure access to the tags for your RDS resources. You can manage access to tags by creating policies for the AddTagsToResource and RemoveTagsFromResource actions. For example, the following policy denies users the ability to add or remove tags for all resources. You can then create policies to allow specific users to add or remove tags.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyTagUpdates",
      "Effect": "Deny",
      "Action": [
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource"
      ],
      "Resource": "*"
    }
  ]
}
```

To see a list of Amazon RDS actions, see [Actions Defined by Amazon RDS in the Service Authorization Reference](#).

Example policies: Using custom tags

Following are examples of how you can use custom tags in Amazon RDS IAM permissions policies. For more information about adding tags to an Amazon RDS resource, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

Note

All examples use the us-west-2 region and contain fictitious account IDs.

Example 1: Grant permission for actions on a resource with a specific tag with two different values

The following policy allows permission to perform the `ModifyDBInstance` and `CreateDBSnapshot` API operations on DB instances with either the stage tag set to development or test.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowDevTestCreate",  
            "Effect": "Allow",  
            "Action": [  
                "rds:ModifyDBInstance",  
                "rds>CreateDBSnapshot"  
            ],  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "rds:db-tag/stage": [  
                        "development",  
                        "test"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

Example 2: Explicitly deny permission to create a DB instance that uses specified DB parameter groups

The following policy explicitly denies permission to create a DB instance that uses DB parameter groups with specific tag values. You might apply this policy if you require that a specific customer-created DB parameter group always be used when creating DB instances. Policies that use Deny are most often used to restrict access that was granted by a broader policy.

Explicitly denying permission supersedes any other permissions granted. This ensures that identities do not accidentally get permission that you never want to grant.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "DenyProductionCreate",  
            "Effect": "Deny",  
            "Action": "rds:CreateDBInstance",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "rds:db-tag/group": ["production"]  
                }  
            }  
        }  
    ]  
}
```

```
        "StringEquals":{  
            "rds:pg-tag/usage":"prod"  
        }  
    }  
}  
]
```

Example 3: Grant permission for actions on a DB instance with an instance name that is prefixed with a user name

The following policy allows permission to call any API (except to AddTagsToResource or RemoveTagsFromResource) on a DB instance that has a DB instance name that is prefixed with the user's name and that has a tag called stage equal to devo or that has no tag called stage.

The Resource line in the policy identifies a resource by its Amazon Resource Name (ARN). For more information about using ARNs with Amazon RDS resources, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

```
{  
    "Version":"2012-10-17",  
    "Statement": [  
        {  
            "Sid":"AllowFullDevAccessNoTags",  
            "Effect":"Allow",  
            "NotAction":[  
                "rds:AddTagsToResource",  
                "rds:RemoveTagsFromResource"  
            ],  
            "Resource":"arn:aws:rds:*:123456789012:db:${aws:username}*",  
            "Condition": {  
                "StringEqualsIfExists": {  
                    "rds:db-tag/stage": "devo"  
                }  
            }  
        }  
    ]  
}
```

AWS managed policies for Amazon RDS

To add permissions to users, groups, and roles, it's easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services don't remove permissions from an AWS managed policy, so policy updates don't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the `ReadOnlyAccess` AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*.

Topics

- [AWS managed policy: `AmazonRDSReadOnlyAccess` \(p. 2036\)](#)
- [AWS managed policy: `AmazonRDSFullAccess` \(p. 2037\)](#)
- [AWS managed policy: `AmazonRDSDataFullAccess` \(p. 2038\)](#)
- [AWS managed policy: `AmazonRDSEnhancedMonitoringRole` \(p. 2039\)](#)
- [AWS managed policy: `AmazonRDSPerformanceInsightsReadOnly` \(p. 2040\)](#)
- [AWS managed policy: `AmazonRDSDirectoryServiceAccess` \(p. 2041\)](#)
- [AWS managed policy: `AmazonRDSServiceRolePolicy` \(p. 2041\)](#)
- [AWS managed policy: `AmazonRDSCustomServiceRolePolicy` \(p. 2042\)](#)

AWS managed policy: `AmazonRDSReadOnlyAccess`

This policy allows read-only access to Amazon RDS through the AWS Management Console.

Permissions details

This policy includes the following permissions:

- `rds` – Allows principals to describe Amazon RDS resources and list the tags for Amazon RDS resources.
- `cloudwatch` – Allows principals to get Amazon CloudWatch metric statistics.
- `ec2` – Allows principals to describe Availability Zones and networking resources.
- `logs` – Allows principals to describe CloudWatch Logs log streams of log groups, and get CloudWatch Logs log events.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "rds:Describe*",  
                "rds>ListTagsForResource",  
                "logs:GetLogEvents",  
                "logs:DescribeLogStreams",  
                "logs:PutLogEvents",  
                "logs:CreateLogStream",  
                "logs:DeleteLogStream",  
                "logs:FilterLogEvents",  
                "logs:PutMetricFilter",  
                "logs:PutRetentionPolicy",  
                "logs:DescribeMetricFilters",  
                "logs:DescribeRetentionPolicy",  
                "logs:DeleteMetricFilter",  
                "logs:DeleteRetentionPolicy"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Action": [
        "cloudwatch:GetMetricStatistics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

AWS managed policy: AmazonRDSFullAccess

This policy provides full access to Amazon RDS through the AWS Management Console.

Permissions details

This policy includes the following permissions:

- **rds** – Allows principals full access to Amazon RDS.
- **application-autoscaling** – Allows principals describe and manage Application Auto Scaling scaling targets and policies.
- **cloudwatch** – Allows principals get CloudWatch metric statics and manage CloudWatch alarms.
- **ec2** – Allows principals to describe Availability Zones and networking resources.
- **logs** – Allows principals to describe CloudWatch Logs log streams of log groups, and get CloudWatch Logs log events.
- **outposts** – Allows principals to get AWS Outposts instance types.
- **pi** – Allows principals to get Performance Insights metrics.
- **sns** – Allows principals to Amazon Simple Notification Service (Amazon SNS) subscriptions and topics, and to publish Amazon SNS messages.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "rds:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricStatistics",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch>DeleteAlarms",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns>ListSubscriptions",
        "sns>ListTopics",
        "sns>Publish",
        "logs>DescribeLogStreams",
        "logs>GetLogEvents",
        "outposts>GetOutpostInstanceTypes"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Action": "pi:*",
    "Effect": "Allow",
    "Resource": "arn:aws:pi:*::metrics/rds/*"
},
{
    "Action": "iam>CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": [
                "rds.amazonaws.com",
                "rds.application-autoscaling.amazonaws.com"
            ]
        }
    }
}
]
```

AWS managed policy: AmazonRDSDDataFullAccess

This policy allows full access to use the Data API and the query editor on Aurora Serverless clusters in a specific AWS account. This policy allows the AWS account to get the value of a secret from AWS Secrets Manager.

You can attach the [AmazonRDSDDataFullAccess](#) policy to your IAM identities.

Permissions details

This policy includes the following permissions:

- **dbqms** – Allows principals to access, create, delete, describe, and update queries. The Database Query Metadata Service (dbqms) is an internal-only service. It provides your recent and saved queries for the query editor on the AWS Management Console for multiple AWS services, including Amazon RDS.
- **rds-data** – Allows principals to run SQL statements on Aurora Serverless databases.

- **secretsmanager** – Allows principals to get the value of a secret from AWS Secrets Manager.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "SecretsManagerDbCredentialsAccess",  
            "Effect": "Allow",  
            "Action": [  
                "secretsmanager:GetSecretValue",  
                "secretsmanager:PutResourcePolicy",  
                "secretsmanager:PutSecretValue",  
                "secretsmanager>DeleteSecret",  
                "secretsmanager:DescribeSecret",  
                "secretsmanager:TagResource"  
            ],  
            "Resource": "arn:aws:secretsmanager:*.*:secret:rds-db-credentials/*"  
        },  
        {  
            "Sid": "RDSDDataServiceAccess",  
            "Effect": "Allow",  
            "Action": [  
                "dbqms>CreateFavoriteQuery",  
                "dbqms:DescribeFavoriteQueries",  
                "dbqms:UpdateFavoriteQuery",  
                "dbqms>DeleteFavoriteQueries",  
                "dbqms:GetQueryString",  
                "dbqms>CreateQueryHistory",  
                "dbqms:DescribeQueryHistory",  
                "dbqms:UpdateQueryHistory",  
                "dbqms>DeleteQueryHistory",  
                "rds-data:ExecuteSql",  
                "rds-data:ExecuteStatement",  
                "rds-data:BatchExecuteStatement",  
                "rds-data:BeginTransaction",  
                "rds-data:CommitTransaction",  
                "rds-data:RollbackTransaction",  
                "secretsmanager>CreateSecret",  
                "secretsmanager>ListSecrets",  
                "secretsmanager:GetRandomPassword",  
                "tag:GetResources"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

AWS managed policy: AmazonRDSEnhancedMonitoringRole

This policy provides access to Amazon CloudWatch Logs for Amazon RDS Enhanced Monitoring.

Permissions details

This policy includes the following permissions:

- **logs** – Allows principals to create CloudWatch Logs log groups and retention policies, and to create and describe CloudWatch Logs log streams of log groups. It also allows principals to put and get CloudWatch Logs log events.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
    {
        "Sid": "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
        "Effect": "Allow",
        "Action": [
            "logs>CreateLogGroup",
            "logs>PutRetentionPolicy"
        ],
        "Resource": [
            "arn:aws:logs:*::log-group:RDS*"
        ]
    },
    {
        "Sid": "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
        "Effect": "Allow",
        "Action": [
            "logs>CreateLogStream",
            "logs>PutLogEvents",
            "logs>DescribeLogStreams",
            "logs>GetLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*::log-group:RDS*:log-stream:*
```

AWS managed policy: [AmazonRDSPerformanceInsightsReadOnly](#)

This policy provides read-only access to Amazon RDS Performance Insights for Amazon RDS DB instances and Amazon Aurora DB clusters.

Permissions details

This policy includes the following permissions:

- **rds** – Allows principals to describe Amazon RDS DB instances and Amazon Aurora DB clusters.
- **pi** – Allows principals make calls to the Amazon RDS Performance Insights API and access Performance Insights metrics.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "rds>DescribeDBInstances",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "rds>DescribeDBClusters",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "pi>DescribeDimensionKeys",
            "Resource": "arn:aws:pi::*:metrics/rds/*"
        }
    ]
}
```

```
{  
    "Effect": "Allow",  
    "Action": "pi:GetDimensionKeyDetails",  
    "Resource": "arn:aws:pi:*.*:metrics/rds/*"  
},  
{  
    "Effect": "Allow",  
    "Action": "pi:GetResourceMetadata",  
    "Resource": "arn:aws:pi:*.*:metrics/rds/*"  
},  
{  
    "Effect": "Allow",  
    "Action": "pi:GetResourceMetrics",  
    "Resource": "arn:aws:pi:*.*:metrics/rds/*"  
},  
{  
    "Effect": "Allow",  
    "Action": "pi>ListAvailableResourceDimensions",  
    "Resource": "arn:aws:pi:*.*:metrics/rds/*"  
},  
{  
    "Effect": "Allow",  
    "Action": "pi>ListAvailableResourceMetrics",  
    "Resource": "arn:aws:pi:*.*:metrics/rds/*"  
}  
]  
}
```

AWS managed policy: AmazonRDSDirectoryServiceAccess

This policy allows Amazon RDS to make calls to the AWS Directory Service.

Permissions details

This policy includes the following permissions:

- ds – Allows principals to describe AWS Directory Service directories and control authorization to AWS Directory Service directories.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": [  
                "ds:DescribeDirectories",  
                "ds:AuthorizeApplication",  
                "ds:UnauthorizeApplication",  
                "ds:GetAuthorizedApplicationDetails"  
            ],  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

AWS managed policy: AmazonRDSServiceRolePolicy

You can't attach the AmazonRDSServiceRolePolicy policy to your IAM entities. This policy is attached to a service-linked role that allows Amazon RDS to perform actions on your behalf. For more information, see [Service-linked role permissions for Amazon RDS \(p. 2089\)](#).

AWS managed policy: AmazonRDSCustomServiceRolePolicy

You can't attach the `AmazonRDSCustomServiceRolePolicy` policy to your IAM entities. This policy is attached to a service-linked role that allows Amazon RDS to perform actions on your behalf. For more information, see [Service-linked role permissions for Amazon RDS Custom \(p. 2093\)](#).

Amazon RDS updates to AWS managed policies

View details about updates to AWS managed policies for Amazon RDS since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon RDS [Document history](#) page.

Change	Description	Date
Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy	<p>Amazon RDS added new permissions to the <code>AmazonRDSCustomServiceRolePolicy</code> of the <code>AWSServiceRoleForRDSCustom</code> service-linked role. RDS Custom supports DB clusters. These new permissions in the policy allow RDS Custom to call AWS services on behalf of your DB clusters.</p> <p>For more information, see Service-linked role permissions for Amazon RDS Custom (p. 2093).</p>	November 9, 2022
Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy	<p>Amazon RDS added new permissions to the <code>AWSServiceRoleForRDS</code> service-linked role for integration with AWS Secrets Manager.</p> <p>Integration with Secrets Manager is required for SQL Server Reporting Services (SSRS) Email to function on RDS. SSRS Email creates a secret on behalf of the customer. The secret uses a reserved naming convention and restricts customer updates.</p> <p>For more information, see Using SSRS Email to send reports (p. 1274).</p>	August 26, 2022
Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy	<p>Amazon RDS added a new Amazon CloudWatch namespace to <code>AmazonRDSPreviewServiceRolePolicy</code> for <code>PutMetricData</code>.</p> <p>This namespace is required for Amazon RDS to publish resource usage metrics.</p> <p>For more information, see Using condition keys to limit access to</p>	June 7, 2022

Change	Description	Date
	<p>CloudWatch namespaces in the Amazon CloudWatch User Guide.</p> <p>Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy</p> <p>Amazon RDS added a new Amazon CloudWatch namespace to <code>AmazonRDSBetaServiceRolePolicy</code> for <code>PutMetricData</code>. This namespace is required for Amazon RDS to publish resource usage metrics. For more information, see Using condition keys to limit access to CloudWatch namespaces in the Amazon CloudWatch User Guide.</p>	June 7, 2022
<p>Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy</p>	<p>Amazon RDS added a new Amazon CloudWatch namespace to <code>AWSServiceRoleForRDS</code> for <code>PutMetricData</code>. This namespace is required for Amazon RDS to publish resource usage metrics. For more information, see Using condition keys to limit access to CloudWatch namespaces in the Amazon CloudWatch User Guide.</p>	April 22, 2022
<p>Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy</p>	<p>Amazon RDS added new permissions to the <code>AWSServiceRoleForRDS</code> service-linked role to manage permissions for customer-owned IP pools and local gateway route tables (LGW-RTBs). These permissions are required for RDS on Outposts to perform Multi-AZ replication across the Outposts' local network. For more information, see Working with Multi-AZ deployments for Amazon RDS on AWS Outposts (p. 911).</p>	April 19, 2022

Change	Description	Date
Identity-based policies (p. 2019) – Update to an existing policy	<p>Amazon RDS added a new permission to the <code>AmazonRDSFullAccess</code> managed policy to describe permissions on LGW-RTBs.</p> <p>This permission is required to describe permissions for RDS on Outposts to perform Multi-AZ replication across the Outposts' local network.</p> <p>For more information, see Working with Multi-AZ deployments for Amazon RDS on AWS Outposts (p. 911).</p>	April 19, 2022
Configuring access policies for Performance Insights (p. 556) – New policy	<p>Amazon RDS added a new service-linked role named <code>AmazonRDSPerformanceInsightsReadOnly</code> to allow Amazon RDS to call AWS services on behalf of your DB instances.</p>	March 10, 2022
Service-linked role permissions for Amazon RDS (p. 2089) – Update to an existing policy	<p>Amazon RDS added new Amazon CloudWatch namespaces to <code>AWSServiceRoleForRDS</code> for <code>PutMetricData</code>.</p> <p>These namespaces are required for Amazon DocumentDB (with MongoDB compatibility) and Amazon Neptune to publish CloudWatch metrics.</p> <p>For more information, see Using condition keys to limit access to CloudWatch namespaces in the Amazon CloudWatch User Guide.</p>	March 4, 2022
Service-linked role permissions for Amazon RDS Custom (p. 2093) – New policy	<p>Amazon RDS added a new service-linked role named <code>AWSServiceRoleForRDSCustom</code> to allow RDS Custom to call AWS services on behalf of your DB instances.</p>	October 26, 2021
Amazon RDS started tracking changes	<p>Amazon RDS started tracking changes for its AWS managed policies.</p>	October 26, 2021

Preventing cross-service confused deputy problems

The *confused deputy problem* is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem.

Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way that it shouldn't have permission to access. To prevent this, AWS provides tools that can help you protect your data for all services with service principals that have been given access to resources in your account. For more information, see [The confused deputy problem](#) in the *IAM User Guide*.

To limit the permissions that Amazon RDS gives another service for a specific resource, we recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies.

In some cases, the `aws:SourceArn` value doesn't contain the account ID, for example when you use the Amazon Resource Name (ARN) for an Amazon S3 bucket. In these cases, make sure to use both global condition context keys to limit permissions. In some cases, you use both global condition context keys and the `aws:SourceArn` value contains the account ID. In these cases, make sure that the `aws:SourceAccount` value and the account in the `aws:SourceArn` use the same account ID when they're used in the same policy statement. If you want only one resource to be associated with the cross-service access, use `aws:SourceArn`. If you want to allow any resource in the specified AWS account to be associated with the cross-service use, use `aws:SourceAccount`.

Make sure that the value of `aws:SourceArn` is an ARN for an Amazon RDS resource type. For more information, see [Working with Amazon Resource Names \(ARNs\) in Amazon RDS \(p. 402\)](#).

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. In some cases, you might not know the full ARN of the resource or you might be specifying multiple resources. In these cases, use the `aws:SourceArn` global context condition key with wildcards (*) for the unknown portions of the ARN. An example is `arn:aws:rds:*:123456789012:*`.

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in Amazon RDS to prevent the confused deputy problem.

```
{  
    "Version": "2012-10-17",  
    "Statement": {  
        "Sid": "ConfusedDeputyPreventionExamplePolicy",  
        "Effect": "Allow",  
        "Principal": {  
            "Service": "rds.amazonaws.com"  
        },  
        "Action": "sts:AssumeRole",  
        "Condition": {  
            "ArnLike": {  
                "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mydbinstance"  
            },  
            "StringEquals": {  
                "aws:SourceAccount": "123456789012"  
            }  
        }  
    }  
}
```

For more examples of policies that use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys, see the following sections:

- [Granting permissions to publish notifications to an Amazon SNS topic \(p. 654\)](#)
- [Manually creating an IAM role for native backup and restore \(p. 1102\)](#)
- [Setting up Windows Authentication for SQL Server DB instances \(p. 1144\)](#)
- [Prerequisites for integrating RDS for SQL Server with S3 \(p. 1154\)](#)
- [Manually creating an IAM role for SQL Server Audit \(p. 1229\)](#)
- [Configuring IAM permissions for RDS for Oracle integration with Amazon S3 \(p. 1648\)](#)
- [Setting up access to an Amazon S3 bucket \(p. 1866\) \(PostgreSQL import\)](#)
- [Setting up access to an Amazon S3 bucket \(p. 1886\) \(PostgreSQL export\)](#)

IAM database authentication for MariaDB, MySQL, and PostgreSQL

You can authenticate to your DB instance using AWS Identity and Access Management (IAM) database authentication. IAM database authentication works with MariaDB, MySQL, and PostgreSQL. With this authentication method, you don't need to use a password when you connect to a DB instance. Instead, you use an authentication token.

An *authentication token* is a unique string of characters that Amazon RDS generates on request. Authentication tokens are generated using AWS Signature Version 4. Each token has a lifetime of 15 minutes. You don't need to store user credentials in the database, because authentication is managed externally using IAM. You can also still use standard database authentication. The token is only used for authentication and doesn't affect the session after it is established.

IAM database authentication provides the following benefits:

- Network traffic to and from the database is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). For more information about using SSL/TLS with Amazon RDS, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).
- You can use IAM to centrally manage access to your database resources, instead of managing access individually on each DB instance.
- For applications running on Amazon EC2, you can use profile credentials specific to your EC2 instance to access your database instead of a password, for greater security.

In general, consider using IAM database authentication when your applications create fewer than 200 connections per second, and you don't want to manage usernames and passwords directly in your application code.

The AWS JDBC Driver for MySQL supports IAM database authentication. For more information, see [AWS IAM Database Authentication](#) in the AWS JDBC Driver for MySQL GitHub repository.

Topics

- [Region and version availability \(p. 2048\)](#)
- [CLI and SDK support \(p. 2048\)](#)
- [Limitations for IAM database authentication \(p. 2049\)](#)
- [Recommendations for IAM database authentication \(p. 2049\)](#)
- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)
- [Connecting to your DB instance using IAM authentication \(p. 2055\)](#)

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability with Amazon RDS and IAM database authentication, see [IAM database authentication \(p. 99\)](#).

CLI and SDK support

IAM database authentication is available for the [AWS CLI](#) and for the following language-specific AWS SDKs:

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go](#)
- [AWS SDK for Java](#)
- [AWS SDK for JavaScript](#)
- [AWS SDK for PHP](#)
- [AWS SDK for Python \(Boto3\)](#)
- [AWS SDK for Ruby](#)

Limitations for IAM database authentication

When using IAM database authentication, the following limitations apply:

- The maximum number of connections per second for your DB instance might be limited depending on its DB instance class and your workload.
- Currently, IAM database authentication doesn't support all global condition context keys.

For more information about global condition context keys, see [AWS global condition context keys](#) in the *IAM User Guide*.

- For PostgreSQL, if the IAM role (`rds_iam`) is added to a user (including the RDS master user), IAM authentication takes precedence over password authentication, so the user must log in as an IAM user.

Recommendations for IAM database authentication

We recommend the following when using IAM database authentication:

- Use IAM database authentication as a mechanism for temporary, personal access to databases.
- Use IAM database authentication when your application requires fewer than 200 new IAM database authentication connections per second.

The database engines that work with Amazon RDS don't impose any limits on authentication attempts per second. However, when you use IAM database authentication, your application must generate an authentication token. Your application then uses that token to connect to the DB instance. If you exceed the limit of maximum new connections per second, then the extra overhead of IAM database authentication can cause connection throttling.

Enabling and disabling IAM database authentication

By default, IAM database authentication is disabled on DB instances. You can enable or disable IAM database authentication using the AWS Management Console, AWS CLI, or the API.

You can enable IAM database authentication when you perform one of the following actions:

- To create a new DB instance with IAM database authentication enabled, see [Creating an Amazon RDS DB instance \(p. 230\)](#).
- To modify a DB instance to enable IAM database authentication, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- To restore a DB instance from a snapshot with IAM database authentication enabled, see [Restoring from a DB snapshot \(p. 452\)](#).
- To restore a DB instance to a point in time with IAM database authentication enabled, see [Restoring a DB instance to a specified time \(p. 499\)](#).

IAM authentication for PostgreSQL DB instances requires that the SSL value be 1. You can't enable IAM authentication for a PostgreSQL DB instance if the SSL value is 0. You can't change the SSL value to 0 if IAM authentication is enabled for a PostgreSQL DB instance.

Console

Each creation or modification workflow has a **Database authentication** section, where you can enable or disable IAM database authentication. In that section, choose **Password and IAM database authentication** to enable IAM database authentication.

To enable or disable IAM database authentication for an existing DB instance

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the DB instance that you want to modify.

Note

Make sure that the DB instance is compatible with IAM authentication. Check the compatibility requirements in [Region and version availability \(p. 2048\)](#).

4. Choose **Modify**.
5. In the **Database authentication** section, choose **Password and IAM database authentication** to enable IAM database authentication.
6. Choose **Continue**.
7. To apply the changes immediately, choose **Immediately** in the **Scheduling of modifications** section.
8. Choose **Modify DB instance**.

AWS CLI

To create a new DB instance with IAM authentication by using the AWS CLI, use the `create-db-instance` command. Specify the `--enable-iam-database-authentication` option, as shown in the following example.

```
aws rds create-db-instance \
--db-instance-identifier mydbinstance \
--db-instance-class db.m3.medium \
--engine MySQL \
--allocated-storage 20 \
--master-username masterawsuser \
--master-user-password masteruserpassword \
--enable-iam-database-authentication
```

To update an existing DB instance to have or not have IAM authentication, use the AWS CLI command `modify-db-instance`. Specify either the `--enable-iam-database-authentication` or `--no-enable-iam-database-authentication` option, as appropriate.

Note

Make sure that the DB instance is compatible with IAM authentication. Check the compatibility requirements in [Region and version availability \(p. 2048\)](#).

By default, Amazon RDS performs the modification during the next maintenance window. If you want to override this and enable IAM DB authentication as soon as possible, use the `--apply-immediately` parameter.

The following example shows how to immediately enable IAM authentication for an existing DB instance.

```
aws rds modify-db-instance \
```

```
--db-instance-identifier mydbinstance \  
--apply-immediately \  
--enable-iam-database-authentication
```

If you are restoring a DB instance, use one of the following AWS CLI commands:

- [restore-db-instance-to-point-in-time](#)
- [restore-db-instance-from-db-snapshot](#)

The IAM database authentication setting defaults to that of the source snapshot. To change this setting, set the `--enable-iam-database-authentication` or `--no-enable-iam-database-authentication` option, as appropriate.

RDS API

To create a new DB instance with IAM authentication by using the API, use the API operation [CreateDBInstance](#). Set the `EnableIAMDatabaseAuthentication` parameter to `true`.

To update an existing DB instance to have IAM authentication, use the API operation [ModifyDBInstance](#). Set the `EnableIAMDatabaseAuthentication` parameter to `true` to enable IAM authentication, or `false` to disable it.

Note

Make sure that the DB instance is compatible with IAM authentication. Check the compatibility requirements in [Region and version availability \(p. 2048\)](#).

If you are restoring a DB instance, use one of the following API operations:

- [RestoreDBInstanceFromDBSnapshot](#)
- [RestoreDBInstanceToPointInTime](#)

The IAM database authentication setting defaults to that of the source snapshot. To change this setting, set the `EnableIAMDatabaseAuthentication` parameter to `true` to enable IAM authentication, or `false` to disable it.

Creating and using an IAM policy for IAM database access

To allow an IAM user or role to connect to your DB instance, you must create an IAM policy. After that, you attach the policy to an IAM user or role.

Note

To learn more about IAM policies, see [Identity and access management for Amazon RDS \(p. 2016\)](#).

The following example policy allows an IAM user to connect to a DB instance using IAM database authentication.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "rds-db:connect"  
            ],  
            "Resource": [  
                "arn:aws:rds:region:account:dbinstance:privilege"  
            ]  
        }  
    ]  
}
```

```
        "arn:aws:rds-db:us-east-2:1234567890:dbuser:db-ABCDEFGHIJKLM01234/db_user"
    }
}
```

Important

A user with administrator permissions can access DB instances without explicit permissions in an IAM policy. If you want to restrict administrator access to DB instances, you can create an IAM role with the appropriate, lesser privileged permissions and assign it to the administrator.

Note

Don't confuse the `rds-db:` prefix with other RDS API operation prefixes that begin with `rds:`. You use the `rds-db:` prefix and the `rds-db:connect` action only for IAM database authentication. They aren't valid in any other context.

The example policy includes a single statement with the following elements:

- **Effect** – Specify Allow to grant access to the DB instance. If you don't explicitly allow access, then access is denied by default.
- **Action** – Specify `rds-db:connect` to allow connections to the DB instance.
- **Resource** – Specify an Amazon Resource Name (ARN) that describes one database account in one DB instance. The ARN format is as follows.

```
arn:aws:rds-db:region:account-id:dbuser:DbiResourceId/db-user-name
```

In this format, replace the following:

- **region** is the AWS Region for the DB instance. In the example policy, the AWS Region is `us-east-2`.
- **account-id** is the AWS account number for the DB instance. In the example policy, the account number is `1234567890`.
- **DbiResourceId** is the identifier for the DB instance. This identifier is unique to an AWS Region and never changes. In the example policy, the identifier is `db-ABCDEFGHIJKLM01234`.

To find a DB instance resource ID in the AWS Management Console for Amazon RDS, choose the DB instance to see its details. Then choose the **Configuration** tab. The **Resource ID** is shown in the **Configuration** section.

Alternatively, you can use the AWS CLI command to list the identifiers and resource IDs for all of your DB instance in the current AWS Region, as shown following.

```
aws rds describe-db-instances --query "DBInstances[*].  
[DBInstanceIdentifier,DbiResourceId]"
```

If you are using Amazon Aurora, specify a `DbClusterResourceId` instead of a `DbiResourceId`. For more information, see [Creating and using an IAM policy for IAM database access](#) in the *Amazon Aurora User Guide*.

Note

If you are connecting to a database through RDS Proxy, specify the proxy resource ID, such as `prx-ABCDEFGHIJKLM01234`. For information about using IAM database authentication with RDS Proxy, see [Connecting to a proxy using IAM authentication \(p. 940\)](#).

- *db-user-name* is the name of the database account to associate with IAM authentication. In the example policy, the database account is db_user.

You can construct other ARNs to support various access patterns. The following policy allows access to two different database accounts in a DB instance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKLM01234/jane_doe",
                "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKLM01234/mary_roe"
            ]
        }
    ]
}
```

The following policy uses the "*" character to match all DB instances and database accounts for a particular AWS account and AWS Region.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:1234567890:dbuser:/*"
            ]
        }
    ]
}
```

The following policy matches all of the DB instances for a particular AWS account and AWS Region. However, the policy only grants access to DB instances that have a *jane_doe* database account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:123456789012:dbuser:*/jane_doe"
            ]
        }
    ]
}
```

}

The IAM user or role has access to only those databases that the database user does. For example, suppose that your DB instance has a database named *dev*, and another database named *test*. If the database user *jane_doe* has access only to *dev*, any IAM users or roles that access that DB instance with the *jane_doe* user also have access only to *dev*. This access restriction is also true for other database objects, such as tables, views, and so on.

An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions. For examples of policies, see [Identity-based policy examples for Amazon RDS \(p. 2025\)](#).

Attaching an IAM policy to an IAM user or role

After you create an IAM policy to allow database authentication, you need to attach the policy to an IAM user or role. For a tutorial on this topic, see [Create and attach your first customer managed policy](#) in the *IAM User Guide*.

As you work through the tutorial, you can use one of the policy examples shown in this section as a starting point and tailor it to your needs. At the end of the tutorial, you have an IAM user with an attached policy that can make use of the `rds-db:connect` action.

Note

You can map multiple IAM users or roles to the same database user account. For example, suppose that your IAM policy specified the following resource ARN.

```
arn:aws:rds-db:us-east-2:123456789012:dbuser:db-12ABC34DEFG5HIJ6KLMN0P78QR/jane_doe
```

If you attach the policy to IAM users *Jane*, *Bob*, and *Diego*, then each of those users can connect to the specified DB instance using the *jane_doe* database account.

Creating a database account using IAM authentication

With IAM database authentication, you don't need to assign database passwords to the user accounts you create. If you remove an IAM user that is mapped to a database account, you should also remove the database account with the `DROP USER` statement.

Note

The user name used for IAM authentication must match the case of the user name in the database.

Topics

- [Using IAM authentication with MariaDB and MySQL \(p. 2054\)](#)
- [Using IAM authentication with PostgreSQL \(p. 2055\)](#)

Using IAM authentication with MariaDB and MySQL

With MariaDB and MySQL, authentication is handled by `AWSAuthenticationPlugin`—an AWS-provided plugin that works seamlessly with IAM to authenticate your IAM users. Connect to the DB instance and issue the `CREATE USER` statement, as shown in the following example.

```
CREATE USER jane_doe IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

The IDENTIFIED WITH clause allows MariaDB and MySQL to use the AWSAuthenticationPlugin to authenticate the database account (jane_doe). The AS 'RDS' clause refers to the authentication method. Make sure the specified database user name is the same as a resource in the IAM policy for IAM database access. For more information, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#).

Note

If you see the following message, it means that the AWS-provided plugin is not available for the current DB instance.

ERROR 1524 (HY000): Plugin 'AWSAuthenticationPlugin' is not loaded
To troubleshoot this error, verify that you are using a supported configuration and that you have enabled IAM database authentication on your DB instance. For more information, see [Region and version availability \(p. 2048\)](#) and [Enabling and disabling IAM database authentication \(p. 2049\)](#).

After you create an account using AWSAuthenticationPlugin, you manage it in the same way as other database accounts. For example, you can modify account privileges with GRANT and REVOKE statements, or modify various account attributes with the ALTER USER statement.

Using IAM authentication with PostgreSQL

To use IAM authentication with PostgreSQL, connect to the DB instance, create database users, and then grant them the rds_iam role as shown in the following example.

```
CREATE USER db_userx;
GRANT rds_iam TO db_userx;
```

Make sure the specified database user name is the same as a resource in the IAM policy for IAM database access. For more information, see [Creating and using an IAM policy for IAM database access \(p. 2051\)](#).

Connecting to your DB instance using IAM authentication

With IAM database authentication, you use an authentication token when you connect to your DB instance. An *authentication token* is a string of characters that you use instead of a password. After you generate an authentication token, it's valid for 15 minutes before it expires. If you try to connect using an expired token, the connection request is denied.

Every authentication token must be accompanied by a valid signature, using AWS signature version 4. (For more information, see [Signature Version 4 signing process](#) in the *AWS General Reference*.) The AWS CLI and an AWS SDK, such as the AWS SDK for Java or AWS SDK for Python (Boto3), can automatically sign each token you create.

You can use an authentication token when you connect to Amazon RDS from another AWS service, such as AWS Lambda. By using a token, you can avoid placing a password in your code. Alternatively, you can use an AWS SDK to programmatically create and programmatically sign an authentication token.

After you have a signed IAM authentication token, you can connect to an Amazon RDS DB instance. Following, you can find out how to do this using either a command line tool or an AWS SDK, such as the AWS SDK for Java or AWS SDK for Python (Boto3).

For more information, see the following blog posts:

- [Use IAM authentication to connect with SQL Workbench/J to Aurora MySQL or Amazon RDS for MySQL](#)
- [Using IAM authentication to connect with pgAdmin Amazon Aurora PostgreSQL or Amazon RDS for PostgreSQL](#)

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

Topics

- [Connecting to your DB instance using IAM authentication from the command line: AWS CLI and mysql client \(p. 2056\)](#)
- [Connecting to your DB instance using IAM authentication from the command line: AWS CLI and psql client \(p. 2058\)](#)
- [Connecting to your DB instance using IAM authentication and the AWS SDK for .NET \(p. 2059\)](#)
- [Connecting to your DB instance using IAM authentication and the AWS SDK for Go \(p. 2062\)](#)
- [Connecting to your DB instance using IAM authentication and the AWS SDK for Java \(p. 2066\)](#)
- [Connecting to your DB instance using IAM authentication and the AWS SDK for Python \(Boto3\) \(p. 2073\)](#)

Connecting to your DB instance using IAM authentication from the command line: AWS CLI and mysql client

You can connect from the command line to an Amazon RDS DB instance with the AWS CLI and mysql command line tool as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

Note

For information about connecting to your database using SQL Workbench/J with IAM authentication, see the blog post [Use IAM authentication to connect with SQL Workbench/J to Aurora MySQL or Amazon RDS for MySQL](#).

Topics

- [Generating an IAM authentication token \(p. 2056\)](#)
- [Connecting to a DB instance \(p. 2057\)](#)

Generating an IAM authentication token

The following example shows how to get a signed authentication token using the AWS CLI.

```
aws rds generate-db-auth-token \
--hostname rdsmysql.123456789012.us-west-2.rds.amazonaws.com \
--port 3306 \
--region us-west-2 \
--username jane_doe
```

In the example, the parameters are as follows:

- --hostname – The host name of the DB instance that you want to access
- --port – The port number used for connecting to your DB instance
- --region – The AWS Region where the DB instance is running
- --username – The database account that you want to access

The first several characters of the token look like the following.

```
rdsmysql.123456789012.us-west-2.rds.amazonaws.com:3306/?Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

Connecting to a DB instance

The general format for connecting is shown following.

```
mysql --host=hostName --port=portNumber --ssl-ca=full_path_to_ssl_certificate --enable-cleartext-plugin --user=userName --password=authToken
```

The parameters are as follows:

- --host – The host name of the DB instance that you want to access
- --port – The port number used for connecting to your DB instance
- --ssl-ca – The full path to the SSL certificate file that contains the public key

For more information about SSL/TLS support for MariaDB, see [Using SSL/TLS with a MariaDB DB instance \(p. 992\)](#).

For more information about SSL/TLS support for MySQL, see [Using SSL/TLS with a MySQL DB instance \(p. 1327\)](#).

To download an SSL certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

- --enable-cleartext-plugin – A value that specifies that AWSAuthenticationPlugin must be used for this connection

If you are using a MariaDB client, the --enable-cleartext-plugin option isn't required.

- --user – The database account that you want to access
- --password – A signed IAM authentication token

The authentication token consists of several hundred characters. It can be unwieldy on the command line. One way to work around this is to save the token to an environment variable, and then use that variable when you connect. The following example shows one way to perform this workaround. In the example, */sample_dir/* is the full path to the SSL certificate file that contains the public key.

```
RDSHOST="mysqlb.123456789012.us-east-1.rds.amazonaws.com"  
TOKEN=$(aws rds generate-db-auth-token --hostname $RDSHOST --port 3306 --region us-west-2  
--username jane_doe )"  
  
mysql --host=$RDSHOST --port=3306 --ssl-ca=/sample_dir/global-bundle.pem --enable-cleartext-plugin --user=jane_doe --password=$TOKEN
```

When you connect using AWSAuthenticationPlugin, the connection is secured using SSL. To verify this, type the following at the mysql> command prompt.

```
show status like 'Ssl%';
```

The following lines in the output show more details.

Variable_name	Value
Ssl_cipher	AES256-SHA
Ssl_version	TLSv1.1
...	...

Connecting to your DB instance using IAM authentication from the command line: AWS CLI and psql client

You can connect from the command line to an Amazon RDS for PostgreSQL DB instance with the AWS CLI and psql command line tool as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

Note

For information about connecting to your database using pgAdmin with IAM authentication, see the blog post [Using IAM authentication to connect with pgAdmin Amazon Aurora PostgreSQL or Amazon RDS for PostgreSQL](#).

Topics

- [Generating an IAM authentication token \(p. 2058\)](#)
- [Connecting to an Amazon RDS PostgreSQL instance \(p. 2059\)](#)

Generating an IAM authentication token

The authentication token consists of several hundred characters so it can be unwieldy on the command line. One way to work around this is to save the token to an environment variable, and then use that variable when you connect. The following example shows how to use the AWS CLI to get a signed authentication token using the generate-db-auth-token command, and store it in a PGASSWORD environment variable.

```
export RDSHOST="rdspostgres.123456789012.us-west-2.rds.amazonaws.com"
export PGPASSWORD=$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --
region us-west-2 --username jane_doe )"
```

In the example, the parameters to the generate-db-auth-token command are as follows:

- **--hostname** – The host name of the DB instance that you want to access
- **--port** – The port number used for connecting to your DB instance
- **--region** – The AWS Region where the DB instance is running
- **--username** – The database account that you want to access

The first several characters of the generated token look like the following.

```
rdspostgres.123456789012.us-west-2.rds.amazonaws.com:5432/?  
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

Connecting to an Amazon RDS PostgreSQL instance

The general format for using psql to connect is shown following.

```
psql "host=hostName port=portNumber sslmode=verify-full  
sslrootcert=full_path_to_ssl_certificate dbname=DBName user=userName password=authToken"
```

The parameters are as follows:

- **host** – The host name of the DB instance that you want to access
- **port** – The port number used for connecting to your DB instance
- **sslmode** – The SSL mode to use

When you use `sslmode=verify-full`, the SSL connection verifies the DB instance endpoint against the endpoint in the SSL certificate.

- **sslrootcert** – The full path to the SSL certificate file that contains the public key

For more information, see [Using SSL with a PostgreSQL DB instance \(p. 1816\)](#).

To download an SSL certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

- **dbname** – The database that you want to access
- **user** – The database account that you want to access
- **password** – A signed IAM authentication token

The following example shows using psql to connect. In the example, psql uses the environment variable `RDSHOST` for the host and the environment variable `PGPASSWORD` for the generated token. Also, `/sample_dir/` is the full path to the SSL certificate file that contains the public key.

```
export RDSHOST="rdspostgres.123456789012.us-west-2.rds.amazonaws.com"  
export PGPASSWORD="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --  
region us-west-2 --username jane_doe )"  
  
psql "host=$RDSHOST port=5432 sslmode=verify-full sslrootcert=/sample_dir/global-bundle.pem  
dbname=DBName user=jane_doe password=$PGPASSWORD"
```

Connecting to your DB instance using IAM authentication and the AWS SDK for .NET

You can connect to an RDS for MariaDB, MySQL, or PostgreSQL DB instance with the AWS SDK for .NET as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

Examples

The following code examples show how to generate an authentication token, and then use it to connect to a DB instance.

To run this code example, you need the [AWS SDK for .NET](#), found on the AWS site. The AWSSDK.CORE and the AWSSDK.RDS packages are required. To connect to a DB instance, use the .NET database connector for the DB engine, such as MySqlConnector for MariaDB or MySQL, or Npgsql for PostgreSQL.

This code connects to a MariaDB or MySQL DB instance.

Modify the values of the following variables as needed:

- `server` – The endpoint of the DB instance that you want to access
- `user` – The database account that you want to access
- `database` – The database that you want to access
- `port` – The port number used for connecting to your DB instance
- `SslMode` – The SSL mode to use

When you use `SslMode=Required`, the SSL connection verifies the DB instance endpoint against the endpoint in the SSL certificate.

- `SslCa` – The full path to the SSL certificate for Amazon RDS

To download a certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

```
using System;
using System.Data;
using MySql.Data;
using MySql.Data.MySqlClient;
using Amazon;

namespace ubuntu
{
    class Program
    {
        static void Main(string[] args)
        {
            var pwd =
Amazon.RDS.Util.RDSSAuthTokenGenerator.GenerateAuthToken(RegionEndpoint.USEast1,
"mysqladb.123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
            // for debug only Console.WriteLine("{0}\n", pwd); //this verifies the token is
generated

        MySqlConnection conn = new MySqlConnection($"server=mysqladb.123456789012.us-
east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;SslCa=Fu
conn.Open();

        // Define a query
        MySqlCommand sampleCommand = new MySqlCommand("SHOW DATABASES;", conn);
    }
}
```

```
// Execute a query
MySqlDataReader mysqlDataRdr = sampleCommand.ExecuteReader();

// Read all rows and output the first column in each row
while (mysqlDataRdr.Read())
    Console.WriteLine(mysqlDataRdr[0]);

mysqlDataRdr.Close();
// Close connection
conn.Close();
}

}
```

This code connects to a PostgreSQL DB instance.

Modify the values of the following variables as needed:

- Server – The endpoint of the DB instance that you want to access
 - User ID – The database account that you want to access
 - Database – The database that you want to access
 - Port – The port number used for connecting to your DB instance
 - SSL Mode – The SSL mode to use

When you use SSL Mode=Required, the SSL connection verifies the DB instance endpoint against the endpoint in the SSL certificate.

- Root Certificate – The full path to the SSL certificate for Amazon RDS

To download a certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

```
using System;
using Npgsql;
using Amazon.RDS.Util;

namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            var pwd =
RDSAuthTokenGenerator.GenerateAuthToken("postgresmydb.123456789012.us-
east-1.rds.amazonaws.com", 5432, "jane_doe");
// for debug only Console.WriteLine("{0}\n", pwd); //this verifies the token is generated

            NpgsqlConnection conn = new
NpgsqlConnection($"Server=postgresmydb.123456789012.us-east-1.rds.amazonaws.com;User
Id=jane_doe;Password={pwd};Database=mydb;SSL Mode=Require;Root
Certificate=full_path_to_ssl_certificate");
            conn.Open();

            // Define a query
            NpgsqlCommand cmd = new NpgsqlCommand("select count(*) FROM pg_user",
conn);

            // Execute a query
            NpgsqlDataReader dr = cmd.ExecuteReader();

            // Read all rows and output the first column in each row
            while (dr.Read())
                Console.WriteLine(dr[0]);
        }
    }
}
```

```
        Console.WriteLine("{0}\n", dr[0]);  
  
        // Close connection  
        conn.Close();  
    }  
}
```

Connecting to your DB instance using IAM authentication and the AWS SDK for Go

You can connect to an RDS for MariaDB, MySQL, or PostgreSQL DB instance with the AWS SDK for Go as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

Examples

To run these code examples, you need the [AWS SDK for Go](#), found on the AWS site.

Modify the values of the following variables as needed:

- dbName – The database that you want to access
- dbUser – The database account that you want to access
- dbHost – The endpoint of the DB instance that you want to access
- dbPort – The port number used for connecting to your DB instance
- region – The AWS Region where the DB instance is running

In addition, make sure the imported libraries in the sample code exist on your system.

Important

The examples in this section use the following code to provide credentials that access a database from a local environment:

```
creds := credentials.NewEnvCredentials()
```

If you are accessing a database from an AWS service, such as Amazon EC2 or Amazon ECS, you can replace the code with the following code:

```
sess := session.Must(session.NewSession())  
creds := sess.Config.Credentials
```

If you make this change, make sure you add the following import:
"github.com/aws/aws-sdk-go/aws/session"

Topics

- [Connecting using IAM authentication and the AWS SDK for Go V2 \(p. 2062\)](#)
- [Connecting using IAM authentication and the AWS SDK for Go V1. \(p. 2064\)](#)

Connecting using IAM authentication and the AWS SDK for Go V2

You can connect to a DB instance using IAM authentication and the AWS SDK for Go V2.

The following code examples show how to generate an authentication token, and then use it to connect to a DB instance.

This code connects to a MariaDB or MySQL DB instance.

```
package main

import (
    "context"
    "database/sql"
    "fmt"

    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
    _ "github.com/go-sql-driver/mysql"
)

func main() {

    var dbName string = "DatabaseName"
    var dbUser string = "DatabaseUser"
    var dbHost string = "mysqladb.123456789012.us-east-1.rds.amazonaws.com"
    var dbPort int = 3306
    var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
    var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
        context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
        panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authenticationToken, dbEndpoint, dbName,
    )

    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

This code connects to a PostgreSQL DB instance.

```
package main

import (
    "context"
    "database/sql"
    "fmt"

    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
    _ "github.com/lib/pq"
```

```

    }

func main() {

    var dbName string = "DatabaseName"
    var dbUser string = "DatabaseUser"
    var dbHost string = "postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
    var dbPort int = 5432
    var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
    var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
        panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
        context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
        panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authenticationToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
}

```

Connecting using IAM authentication and the AWS SDK for Go V1.

You can connect to a DB instance using IAM authentication and the AWS SDK for Go V1

The following code examples show how to generate an authentication token, and then use it to connect to a DB instance.

This code connects to a MariaDB or MySQL DB instance.

```

package main

import (
    "database/sql"
    "fmt"
    "log"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
    _ "github.com/go-sql-driver/mysql"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mysqlDb.123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 3306
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
}

```

```

region := "us-east-1"

creds := credentials.NewEnvCredentials()
authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
if err != nil {
    panic(err)
}

dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
    dbUser, authToken, dbEndpoint, dbName,
)

db, err := sql.Open("mysql", dsn)
if err != nil {
    panic(err)
}

err = db.Ping()
if err != nil {
    panic(err)
}
}
}

```

This code connects to a PostgreSQL DB instance.

```

package main

import (
    "database/sql"
    "fmt"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
    _ "github.com/lib/pq"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 5432
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
    region := "us-east-1"

    creds := credentials.NewEnvCredentials()
    authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
    if err != nil {
        panic(err)
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
}

```

Connecting to your DB instance using IAM authentication and the AWS SDK for Java

You can connect to an RDS for MariaDB, MySQL, or PostgreSQL DB instance with the AWS SDK for Java as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)
- [Set up the AWS SDK for Java](#)

Topics

- [Generating an IAM authentication token \(p. 2066\)](#)
- [Manually constructing an IAM authentication token \(p. 2067\)](#)
- [Connecting to a DB instance \(p. 2070\)](#)

Generating an IAM authentication token

If you are writing programs using the AWS SDK for Java, you can get a signed authentication token using the `RdsIamAuthTokenGenerator` class. Using this class requires that you provide AWS credentials. To do this, you create an instance of the `DefaultAWSCredentialsProviderChain` class. `DefaultAWSCredentialsProviderChain` uses the first AWS access key and secret key that it finds in the [default credential provider chain](#). For more information about AWS access keys, see [Managing access keys for IAM users](#).

After you create an instance of `RdsIamAuthTokenGenerator`, you can call the `getAuthToken` method to obtain a signed token. Provide the AWS Region, host name, port number, and user name. The following code example illustrates how to do this.

```
package com.amazonaws.codesamples;

import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;

public class GenerateRDSAuthToken {

    public static void main(String[] args) {

        String region = "us-west-2";
        String hostname = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
        String port = "3306";
        String username = "jane_doe";

        System.out.println(generateAuthToken(region, hostname, port, username));
    }

    static String generateAuthToken(String region, String hostName, String port, String
username) {

        RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
            .credentials(new DefaultAWSCredentialsProviderChain())
            .region(region)
    }
}
```

```

        .build();

    String authToken = generator.getAuthToken(
        GetIamAuthTokenRequest.builder()
            .hostname(hostName)
            .port(Integer.parseInt(port))
            .userName(username)
            .build());

    return authToken;
}

}

```

Manually constructing an IAM authentication token

In Java, the easiest way to generate an authentication token is to use `RdsIamAuthTokenGenerator`. This class creates an authentication token for you, and then signs it using AWS signature version 4. For more information, see [Signature version 4 signing process](#) in the *AWS General Reference*.

However, you can also construct and sign an authentication token manually, as shown in the following code example.

```

package com.amazonaws.codesamples;

import com.amazonaws.SdkClientException;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.SigningAlgorithm;
import com.amazonaws.util.BinaryUtils;
import org.apache.commons.lang3.StringUtils;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.Charset;
import java.security.MessageDigest;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.SortedMap;
import java.util.TreeMap;

import static com.amazonaws.auth.internal.SignerConstants.AWS4_TERMINATOR;
import static com.amazonaws.util.StringUtils.UTF8;

public class CreateRDSAAuthTokenManually {
    public static String httpMethod = "GET";
    public static String action = "connect";
    public static String canonicalURIParameter = "/";
    public static SortedMap<String, String> canonicalQueryParameters = new TreeMap();
    public static String payload = StringUtils.EMPTY;
    public static String signedHeader = "host";
    public static String algorithm = "AWS4-HMAC-SHA256";
    public static String serviceName = "rds-db";
    public static String requestWithoutSignature;

    public static void main(String[] args) throws Exception {

        String region = "us-west-2";
        String instanceName = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
        String port = "3306";
        String username = "jane_doe";

        Date now = new Date();
        String date = new SimpleDateFormat("yyyyMMdd").format(now);
        String dateTimeStamp = new SimpleDateFormat("yyyyMMdd'T'HHmmss'Z'").format(now);

```

```

        DefaultAWSCredentialsProviderChain creds = new
DefaultAWSCredentialsProviderChain();
        String awsAccessKey = creds.getCredentials().getAWSAccessKeyId();
        String awsSecretKey = creds.getCredentials().getAWSSecretKey();
        String expiryMinutes = "900";

        System.out.println("Step 1: Create a canonical request:");
        String canonicalString = createCanonicalString(username, awsAccessKey, date,
dateTimeStamp, region, expiryMinutes, instanceName, port);
        System.out.println(canonicalString);
        System.out.println();

        System.out.println("Step 2: Create a string to sign:");
        String stringToSign = createStringToSign(dateTimeStamp, canonicalString,
awsAccessKey, date, region);
        System.out.println(stringToSign);
        System.out.println();

        System.out.println("Step 3: Calculate the signature:");
        String signature = BinaryUtils.toHex(calculateSignature(stringToSign,
newSigningKey(awsSecretKey, date, region, serviceName)));
        System.out.println(signature);
        System.out.println();

        System.out.println("Step 4: Add the signing info to the request");
        System.out.println	appendSignature(signature));
        System.out.println();

    }

    //Step 1: Create a canonical request date should be in format YYYYMMDD and date
    //Time should be in format YYYYMMDDTHHMMSSZ
    public static String createCanonicalString(String user, String accessKey, String date,
String dateTime, String region, String expiryPeriod, String hostName, String port) throws
Exception {
        canonicalQueryParameters.put("Action", action);
        canonicalQueryParameters.put("DBUser", user);
        canonicalQueryParameters.put("X-Amz-Algorithm", "AWS4-HMAC-SHA256");
        canonicalQueryParameters.put("X-Amz-Credential", accessKey + "%2F" + date + "%2F" +
region + "%2F" + serviceName + "%2Faws4_request");
        canonicalQueryParameters.put("X-Amz-Date", dateTime);
        canonicalQueryParameters.put("X-Amz-Expires", expiryPeriod);
        canonicalQueryParameters.put("X-Amz-SignedHeaders", signedHeader);
        String canonicalQueryString = "";
        while(!canonicalQueryParameters.isEmpty()) {
            String currentQueryParameter = canonicalQueryParameters.firstKey();
            String currentQueryParameterValue =
canonicalQueryParameters.remove(currentQueryParameter);
            canonicalQueryString = canonicalQueryString + currentQueryParameter + "=" +
currentQueryParameterValue;
            if (!currentQueryParameter.equals("X-Amz-SignedHeaders")) {
                canonicalQueryString += "&";
            }
        }
        String canonicalHeaders = "host:" + hostName + ":" + port + '\n';
        requestWithoutSignature = hostName + ":" + port + "/" + canonicalQueryString;

        String hashedPayload = BinaryUtils.toHex(hash(payload));
        return httpMethod + '\n' + canonicalURIParameter + '\n' + canonicalQueryString +
'\n' + canonicalHeaders + '\n' + signedHeader + '\n' + hashedPayload;
    }

    //Step 2: Create a string to sign using sig v4
    public static String createStringToSign(String dateTime, String canonicalRequest,
String accessKey, String date, String region) throws Exception {

```

```

String credentialScope = date + "/" + region + "/" + serviceName + "/aws4_request";
return algorithm + '\n' + date + '\n' + credentialScope + '\n' +
BinaryUtils.toHex(hash(canonicalRequest));

}

//Step 3: Calculate signature
/**
 * Step 3 of the &AWS; Signature version 4 calculation. It involves deriving
 * the signing key and computing the signature. Refer to
 * http://docs.aws.amazon
 * .com/general/latest/gr/sigv4-calculate-signature.html
 */
public static byte[] calculateSignature(String stringToSign,
                                         byte[] signingKey) {
    return sign(stringToSign.getBytes(Charset.forName("UTF-8")), signingKey,
               SigningAlgorithm.HmacSHA256);
}

public static byte[] sign(byte[] data, byte[] key,
                         SigningAlgorithm algorithm) throwsSdkClientException {
    try {
        Mac mac = algorithm.getMac();
        mac.init(new SecretKeySpec(key, algorithm.toString()));
        return mac.doFinal(data);
    } catch (Exception e) {
        throw new SdkClientException(
            "Unable to calculate a request signature: "
            + e.getMessage(), e);
    }
}

public static byte[] newSigningKey(String secretKey,
                                   String dateStamp, String regionName, String serviceName)
{
    byte[] kSecret = ("AWS4" + secretKey).getBytes(Charset.forName("UTF-8"));
    byte[] kDate = sign(dateStamp, kSecret, SigningAlgorithm.HmacSHA256);
    byte[] kRegion = sign(regionName, kDate, SigningAlgorithm.HmacSHA256);
    byte[] kService = sign(serviceName, kRegion,
                           SigningAlgorithm.HmacSHA256);
    return sign(AWS4_TERMINATOR, kService, SigningAlgorithm.HmacSHA256);
}

public static byte[] sign(String stringData, byte[] key,
                         SigningAlgorithm algorithm) throwsSdkClientException {
    try {
        byte[] data = stringData.getBytes(UTF8);
        return sign(data, key, algorithm);
    } catch (Exception e) {
        throw new SdkClientException(
            "Unable to calculate a request signature: "
            + e.getMessage(), e);
    }
}

//Step 4: append the signature
public static String appendSignature(String signature) {
    return requestWithoutSignature + "&X-Amz-Signature=" + signature;
}

public static byte[] hash(String s) throws Exception {
    try {
        MessageDigest md = MessageDigest.getInstance("SHA-256");
        md.update(s.getBytes(UTF8));
        return md.digest();
    } catch (Exception e) {

```

```
        throw new SdkClientException(
            "Unable to compute hash while signing request: "
            + e.getMessage(), e);
    }
}
```

Connecting to a DB instance

The following code example shows how to generate an authentication token, and then use it to connect to an instance running MariaDB or MySQL.

To run this code example, you need the [AWS SDK for Java](#), found on the AWS site. In addition, you need the following:

- MySQL Connector/J. This code example was tested with mysql-connector-java-5.1.33-bin.jar.
- An intermediate certificate for Amazon RDS that is specific to an AWS Region. (For more information, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).) At runtime, the class loader looks for the certificate in the same directory as this Java code example, so that the class loader can find it.
- Modify the values of the following variables as needed:
 - RDS_INSTANCE_HOSTNAME – The host name of the DB instance that you want to access.
 - RDS_INSTANCE_PORT – The port number used for connecting to your PostgreSQL DB instance.
 - REGION_NAME – The AWS Region where the DB instance is running.
 - DB_USER – The database account that you want to access.
 - SSL_CERTIFICATE – An SSL certificate for Amazon RDS that is specific to an AWS Region.

To download a certificate for your AWS Region, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#). Place the SSL certificate in the same directory as this Java program file, so that the class loader can find the certificate at runtime.

This code example obtains AWS credentials from the [default credential provider chain](#).

```
package com.amazonaws.samples;

import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.AWSStaticCredentialsProvider;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.security.KeyStore;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;
import java.util.Properties;

import java.net.URL;

public class IAMDatabaseAuthenticationTester {
```

```

//&AWS; Credentials of the IAM user with policy enabling IAM Database Authenticated
access to the db by the db user.
private static final DefaultAWSCredentialsProviderChain creds = new
DefaultAWSCredentialsProviderChain();
private static final String AWS_ACCESS_KEY =
creds.getCredentials().getAWSAccessKeyId();
private static final String AWS_SECRET_KEY = creds.getCredentials().getAWSSecretKey();

//Configuration parameters for the generation of the IAM Database Authentication token
private static final String RDS_INSTANCE_HOSTNAME = "rdsmysql.123456789012.us-
west-2.rds.amazonaws.com";
private static final int RDS_INSTANCE_PORT = 3306;
private static final String REGION_NAME = "us-west-2";
private static final String DB_USER = "jane_doe";
private static final String JDBC_URL = "jdbc:mysql://" + RDS_INSTANCE_HOSTNAME + ":" +
RDS_INSTANCE_PORT;

private static final String SSL_CERTIFICATE = "rds-ca-2019-us-west-2.pem";

private static final String KEY_STORE_TYPE = "JKS";
private static final String KEY_STORE_PROVIDER = "SUN";
private static final String KEY_STORE_FILE_PREFIX = "sys-connect-via-ssl-test-cacerts";
private static final String KEY_STORE_FILE_SUFFIX = ".jks";
private static final String DEFAULT_KEY_STORE_PASSWORD = "changeit";

public static void main(String[] args) throws Exception {
    //get the connection
    Connection connection = getDBConnectionUsingIam();

    //verify the connection is successful
    Statement stmt= connection.createStatement();
    ResultSet rs=stmt.executeQuery("SELECT 'Success!' FROM DUAL;");
    while (rs.next()) {
        String id = rs.getString(1);
        System.out.println(id); //Should print "Success!"
    }

    //close the connection
    stmt.close();
    connection.close();

    clearSslProperties();
}

/**
 * This method returns a connection to the db instance authenticated using IAM Database
Authentication
 * @return
 * @throws Exception
 */
private static Connection getDBConnectionUsingIam() throws Exception {
    setSslProperties();
    return DriverManager.getConnection(JDBC_URL, setMySqlConnectionProperties());
}

/**
 * This method sets the mysql connection properties which includes the IAM Database
Authentication token
 * as the password. It also specifies that SSL verification is required.
 * @return
 */
private static Properties setMySqlConnectionProperties() {
    Properties mysqlConnectionProperties = new Properties();
    mysqlConnectionProperties.setProperty("verifyServerCertificate","true");
    mysqlConnectionProperties.setProperty("useSSL", "true");
}

```

```

        mysqlConnectionProperties.setProperty("user",DB_USER);
        mysqlConnectionProperties.setProperty("password",generateAuthToken());
        return mysqlConnectionProperties;
    }

    /**
     * This method generates the IAM Auth Token.
     * An example IAM Auth Token would look like follows:
     * btusi123.cmz7kenwo2ye.rds.cn-north-1.amazonaws.com.cn:3306/?Action=connect&DBUser=iamtestuser&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20171003T010726Z&X-Amz-SignedHeaders=host&X-Amz-Expires=899&X-Amz-Credential=AKIAPFXHGVDI5RNF04AQ%2F20171003%2Fcna-north-1%2Frds-db%2Faws4_request&X-Amz-Signature=f9f45ef96c1f770cdad11a53e33ffa4c3730bc03fdee820cfdf1322eed15483b
     * @return
     */
    private static String generateAuthToken() {
        BasicAWSCredentials awsCredentials = new BasicAWSCredentials(AWS_ACCESS_KEY,
        AWS_SECRET_KEY);

        RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
            .credentials(new
        AWSStaticCredentialsProvider(awsCredentials)).region(REGION_NAME).build();
        return generator.getAuthToken(GetIamAuthTokenRequest.builder()

.hostname(RDS_INSTANCE_HOSTNAME).port(RDS_INSTANCE_PORT).userName(DB_USER).build());
    }

    /**
     * This method sets the SSL properties which specify the key store file, its type and
password:
     * @throws Exception
     */
    private static void setSslProperties() throws Exception {
        System.setProperty("javax.net.ssl.trustStore", createKeyStoreFile());
        System.setProperty("javax.net.ssl.trustStoreType", KEY_STORE_TYPE);
        System.setProperty("javax.net.ssl.trustStorePassword", DEFAULT_KEY_STORE_PASSWORD);
    }

    /**
     * This method returns the path of the Key Store File needed for the SSL verification
during the IAM Database Authentication to
     * the db instance.
     * @return
     * @throws Exception
     */
    private static String createKeyStoreFile() throws Exception {
        return createKeyStoreFile(createCertificate()).getPath();
    }

    /**
     * This method generates the SSL certificate
     * @return
     * @throws Exception
     */
    private static X509Certificate createCertificate() throws Exception {
        CertificateFactory certFactory = CertificateFactory.getInstance("X.509");
        URL url = new File(SSL_CERTIFICATE).toURI().toURL();
        if (url == null) {
            throw new Exception();
        }
        try (InputStream certInputStream = url.openStream()) {
            return (X509Certificate) certFactory.generateCertificate(certInputStream);
        }
    }

    /**

```

```
* This method creates the Key Store File
* @param rootX509Certificate - the SSL certificate to be stored in the KeyStore
* @return
* @throws Exception
*/
private static File createKeyStoreFile(X509Certificate rootX509Certificate) throws
Exception {
    File keyStoreFile = File.createTempFile(KEY_STORE_FILE_PREFIX,
KEY_STORE_FILE_SUFFIX);
    try (FileOutputStream fos = new FileOutputStream(keyStoreFile.getPath())) {
        KeyStore ks = KeyStore.getInstance(KEY_STORE_TYPE, KEY_STORE_PROVIDER);
        ks.load(null);
        ks.setCertificateEntry("rootCaCertificate", rootX509Certificate);
        ks.store(fos, DEFAULT_KEY_STORE_PASSWORD.toCharArray());
    }
    return keyStoreFile;
}

/**
 * This method clears the SSL properties.
 * @throws Exception
*/
private static void clearSslProperties() throws Exception {
    System.clearProperty("javax.net.ssl.trustStore");
    System.clearProperty("javax.net.ssl.trustStoreType");
    System.clearProperty("javax.net.ssl.trustStorePassword");
}
}
```

Connecting to your DB instance using IAM authentication and the AWS SDK for Python (Boto3)

You can connect to an RDS for MariaDB, MySQL, or PostgreSQL DB instance with the AWS SDK for Python (Boto3) as described following.

Prerequisites

The following are prerequisites for connecting to your DB instance using IAM authentication:

- [Enabling and disabling IAM database authentication \(p. 2049\)](#)
- [Creating and using an IAM policy for IAM database access \(p. 2051\)](#)
- [Creating a database account using IAM authentication \(p. 2054\)](#)

In addition, make sure the imported libraries in the sample code exist on your system.

Examples

The code examples use profiles for shared credentials. For information about specifying credentials, see [Credentials](#) in the AWS SDK for Python (Boto3) documentation.

The following code examples show how to generate an authentication token, and then use it to connect to a DB instance.

To run this code example, you need the [AWS SDK for Python \(Boto3\)](#), found on the AWS site.

Modify the values of the following variables as needed:

- ENDPOINT – The endpoint of the DB instance that you want to access
- PORT – The port number used for connecting to your DB instance

- USER – The database account that you want to access
- REGION – The AWS Region where the DB instance is running
- DBNAME – The database that you want to access
- SSLCERTIFICATE – The full path to the SSL certificate for Amazon RDS

For `ssl_ca`, specify an SSL certificate. To download an SSL certificate, see [Using SSL/TLS to encrypt a connection to a DB instance \(p. 2005\)](#).

This code connects to a MariaDB or MySQL DB instance.

Before running this code, install Connector/Python version 8.0 by following the instructions in [Connector/Python Installation](#) in the MySQL documentation.

```
import mysql.connector
import sys
import boto3
import os

ENDPOINT="mysqladb.123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"
os.environ['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='default')
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
Region=REGION)

try:
    conn = mysql.connector.connect(host=ENDPOINT, user=USER, passwd=token, port=PORT,
database=DBNAME, ssl_ca='SSLCERTIFICATE')
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

This code connects to a PostgreSQL DB instance.

Before running this code, install psycopg2 by following the instructions in [Psycopg documentation](#).

```
import psycopg2
import sys
import boto3
import os

ENDPOINT="postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
```

```
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
Region=REGION)

try:
    conn = psycopg2.connect(host=ENDPOINT, port=PORT, database=DBNAME, user=USER,
password=token, sslrootcert="SSLCERTIFICATE")
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

Troubleshooting Amazon RDS identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon RDS and IAM.

Topics

- [I'm not authorized to perform an action in Amazon RDS \(p. 2075\)](#)
- [I'm not authorized to perform iam:PassRole \(p. 2075\)](#)
- [I want to view my access keys \(p. 2076\)](#)
- [I'm an administrator and want to allow others to access Amazon RDS \(p. 2076\)](#)
- [I want to allow people outside of my AWS account to access my Amazon RDS resources \(p. 2076\)](#)

I'm not authorized to perform an action in Amazon RDS

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the mateojackson IAM user tries to use the console to view details about a `widget` but does not have `rds:GetWidget` permissions.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
rds:GetWidget on resource: my-example-widget
```

In this case, Mateo asks his administrator to update his policies to allow him to access the `my-example-widget` resource using the `rds:GetWidget` action.

I'm not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Amazon RDS.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon RDS. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

Important

Do not provide your access keys to a third party, even to help [find your canonical user ID](#). By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see [Managing access keys](#) in the *IAM User Guide*.

I'm an administrator and want to allow others to access Amazon RDS

To enable others to access Amazon RDS, you must create an IAM entity (user or role) for the person or application that needs access. They use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon RDS.

To get started right away, see [Creating your first IAM delegated user and group](#) in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Amazon RDS resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon RDS supports these features, see [How Amazon RDS works with IAM \(p. 2020\)](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](#) in the *IAM User Guide*.

Logging and monitoring in Amazon RDS

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon RDS and your AWS solutions. You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multi-point failure if one occurs. AWS provides several tools for monitoring your Amazon RDS resources and responding to potential incidents:

Amazon CloudWatch Alarms

Using Amazon CloudWatch alarms, you watch a single metric over a time period that you specify. If the metric exceeds a given threshold, a notification is sent to an Amazon SNS topic or AWS Auto Scaling policy. CloudWatch alarms do not invoke actions because they are in a particular state. Rather the state must have changed and been maintained for a specified number of periods.

AWS CloudTrail Logs

CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon RDS. CloudTrail captures all API calls for Amazon RDS as events, including calls from the console and from code calls to Amazon RDS API operations. Using the information collected by CloudTrail, you can determine the request that was made to Amazon RDS, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see [Monitoring Amazon RDS API calls in AWS CloudTrail \(p. 725\)](#).

Enhanced Monitoring

Amazon RDS provides metrics in real time for the operating system (OS) that your DB instance runs on. You can view the metrics for your DB instance using the console, or consume the Enhanced Monitoring JSON output from Amazon CloudWatch Logs in a monitoring system of your choice. For more information, see [Monitoring OS metrics with Enhanced Monitoring \(p. 600\)](#).

Amazon RDS Performance Insights

Performance Insights expands on existing Amazon RDS monitoring features to illustrate your database's performance and help you analyze any issues that affect it. With the Performance Insights dashboard, you can visualize the database load and filter the load by waits, SQL statements, hosts, or users. For more information, see [Monitoring DB load with Performance Insights on Amazon RDS \(p. 543\)](#).

Database Logs

You can view, download, and watch database logs using the AWS Management Console, AWS CLI, or RDS API. For more information, see [Monitoring Amazon RDS log files \(p. 680\)](#).

Amazon RDS Recommendations

Amazon RDS provides automated recommendations for database resources. These recommendations provide best practice guidance by analyzing DB instance configuration, usage, and performance data. For more information, see [Viewing Amazon RDS recommendations \(p. 520\)](#).

Amazon RDS Event Notification

Amazon RDS uses the Amazon Simple Notification Service (Amazon SNS) to provide notification when an Amazon RDS event occurs. These notifications can be in any notification form supported by Amazon SNS for an AWS Region, such as an email, a text message, or a call to an HTTP endpoint. For more information, see [Working with Amazon RDS event notification \(p. 650\)](#).

AWS Trusted Advisor

Trusted Advisor draws upon best practices learned from serving hundreds of thousands of AWS customers. Trusted Advisor inspects your AWS environment and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps. All AWS customers have access to five Trusted Advisor checks. Customers with a Business or Enterprise support plan can view all Trusted Advisor checks.

Trusted Advisor has the following Amazon RDS-related checks:

- Amazon RDS Idle DB Instances
- Amazon RDS Security Group Access Risk
- Amazon RDS Backups
- Amazon RDS Multi-AZ

For more information on these checks, see [Trusted Advisor best practices \(checks\)](#).

For more information about monitoring Amazon RDS, see [Monitoring metrics in an Amazon RDS instance \(p. 510\)](#).

Compliance validation for Amazon RDS

Third-party auditors assess the security and compliance of Amazon RDS as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see [AWS services in scope by compliance program](#). For general information, see [AWS compliance programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading reports in AWS Artifact](#).

Your compliance responsibility when using Amazon RDS is determined by the sensitivity of your data, your organization's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and compliance quick start guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA security and compliance whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- [AWS compliance resources](#) – This collection of workbooks and guides that might apply to your industry and location.
- [AWS Config](#) – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon RDS

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS global infrastructure](#).

In addition to the AWS global infrastructure, Amazon RDS offers features to help support your data resiliency and backup needs.

Backup and restore

Amazon RDS creates and saves automated backups of your DB instance. Amazon RDS creates a storage volume snapshot of your DB instance, backing up the entire DB instance and not just individual databases.

Amazon RDS creates automated backups of your DB instance during the backup window of your DB instance. Amazon RDS saves the automated backups of your DB instance according to the backup retention period that you specify. If necessary, you can recover your database to any point in time during the backup retention period. You can also back up your DB instance manually, by manually creating a DB snapshot.

You can create a DB instance by restoring from this DB snapshot as a disaster recovery solution if the source DB instance fails.

For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

Replication

Amazon RDS uses the MariaDB, MySQL, Oracle, and PostgreSQL DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Using read replicas, you can elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads. You can promote a read replica to a standalone instance as a disaster recovery solution if the source DB instance fails. For some DB engines, Amazon RDS also supports other replication options.

For more information, see [Working with read replicas \(p. 370\)](#).

Failover

Amazon RDS provides high availability and failover support for DB instances using Multi-AZ deployments. Amazon RDS uses several different technologies to provide failover support. Multi-AZ deployments for Oracle, PostgreSQL, MySQL, and MariaDB DB instances use Amazon's failover technology. SQL Server DB instances use SQL Server Database Mirroring (DBM).

For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).

Infrastructure security in Amazon RDS

As a managed service, Amazon RDS is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of security processes](#) whitepaper.

You use AWS published API calls to access Amazon RDS through the network. Clients must support Transport Layer Security (TLS) 1.0. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the [AWS Security Token Service \(AWS STS\)](#) to generate temporary security credentials to sign requests.

In addition, Amazon RDS offers features to help support infrastructure security.

Security groups

Security groups control the access that traffic has in and out of a DB instance. By default, network access is turned off to a DB instance. You can specify rules in a security group that allow access from an IP address range, port, or security group. After ingress rules are configured, the same rules apply to all DB instances that are associated with that security group.

For more information, see [Controlling access with security groups \(p. 2085\)](#).

Public accessibility

When you launch a DB instance inside a virtual private cloud (VPC) based on the Amazon VPC service, you can turn on or off public accessibility for that DB instance. To designate whether the DB instance that you create has a DNS name that resolves to a public IP address, you use the *Public accessibility* parameter. By using this parameter, you can designate whether there is public access to the DB instance. You can modify a DB instance to turn on or off public accessibility by modifying the *Public accessibility* parameter.

For more information, see [Hiding a DB instance in a VPC from the internet \(p. 2109\)](#).

Note

If your DB instance is in a VPC but isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see [Internetwork traffic privacy \(p. 2015\)](#).

Amazon RDS API and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and Amazon RDS API endpoints by creating an *interface VPC endpoint*. Interface endpoints are powered by [AWS PrivateLink](#).

AWS PrivateLink enables you to privately access Amazon RDS API operations without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. DB instances in your VPC don't need public IP addresses to communicate with Amazon RDS API endpoints to launch, modify, or terminate DB instances. Your DB instances also don't need public IP addresses to use any of the available RDS API operations. Traffic between your VPC and Amazon RDS doesn't leave the Amazon network.

Each interface endpoint is represented by one or more elastic network interfaces in your subnets. For more information on elastic network interfaces, see [Elastic network interfaces](#) in the *Amazon EC2 User Guide*.

For more information about VPC endpoints, see [Interface VPC endpoints \(AWS PrivateLink\)](#) in the *Amazon VPC User Guide*. For more information about RDS API operations, see [Amazon RDS API Reference](#).

You don't need an interface VPC endpoint to connect to a DB instance. For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

Considerations for VPC endpoints

Before you set up an interface VPC endpoint for Amazon RDS API endpoints, ensure that you review [Interface endpoint properties and limitations](#) in the *Amazon VPC User Guide*.

All RDS API operations relevant to managing Amazon RDS resources are available from your VPC using AWS PrivateLink.

VPC endpoint policies are supported for RDS API endpoints. By default, full access to RDS API operations is allowed through the endpoint. For more information, see [Controlling access to services with VPC endpoints](#) in the *Amazon VPC User Guide*.

Availability

Amazon RDS API currently supports VPC endpoints in the following AWS Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)

- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europe (Milan)
- Middle East (Bahrain)
- South America (São Paulo)
- China (Beijing)
- China (Ningxia)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Creating an interface VPC endpoint for Amazon RDS API

You can create a VPC endpoint for the Amazon RDS API using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see [Creating an interface endpoint](#) in the *Amazon VPC User Guide*.

Create a VPC endpoint for Amazon RDS API using the service name com.amazonaws.*region*.rds.

Excluding AWS Regions in China, if you enable private DNS for the endpoint, you can make API requests to Amazon RDS with the VPC endpoint using its default DNS name for the AWS Region, for example rds.us-east-1.amazonaws.com. For the China (Beijing) and China (Ningxia) AWS Regions, you can make API requests with the VPC endpoint using rds-api.cn-north-1.amazonaws.com.cn and rds-api.cn-northwest-1.amazonaws.com.cn, respectively.

For more information, see [Accessing a service through an interface endpoint](#) in the *Amazon VPC User Guide*.

Creating a VPC endpoint policy for Amazon RDS API

You can attach an endpoint policy to your VPC endpoint that controls access to Amazon RDS API. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see [Controlling access to services with VPC endpoints](#) in the *Amazon VPC User Guide*.

Example: VPC endpoint policy for Amazon RDS API actions

The following is an example of an endpoint policy for Amazon RDS API. When attached to an endpoint, this policy grants access to the listed Amazon RDS API actions for all principals on all resources.

```
{  
    "Statement": [  
        {  
            "Principal": "*",  
            "Action": "rds:  
                *",  
            "Effect": "Allow",  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "Effect": "Allow",
        "Action": [
            "rds:CreateDBInstance",
            "rds:ModifyDBInstance",
            "rds>CreateDBSnapshot"
        ],
        "Resource": "*"
    }
}
```

Example: VPC endpoint policy that denies all access from a specified AWS account

The following VPC endpoint policy denies AWS account 123456789012 all access to resources using the endpoint. The policy allows all actions from other accounts.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Security best practices for Amazon RDS

Use AWS Identity and Access Management (IAM) accounts to control access to Amazon RDS API operations, especially operations that create, modify, or delete Amazon RDS resources. Such resources include DB instances, security groups, and parameter groups. Also use IAM to control actions that perform common administrative actions such as backing up and restoring DB instances.

- Create an individual IAM user for each person who manages Amazon RDS resources, including yourself. Don't use AWS root credentials to manage Amazon RDS resources.
- Grant each user the minimum set of permissions required to perform his or her duties.
- Use IAM groups to effectively manage permissions for multiple users.
- Rotate your IAM credentials regularly.
- Configure AWS Secrets Manager to automatically rotate the secrets for Amazon RDS. For more information, see [Rotating your AWS Secrets Manager secrets](#) in the *AWS Secrets Manager User Guide*. You can also retrieve the credential from AWS Secrets Manager programmatically. For more information, see [Retrieving the secret value](#) in the *AWS Secrets Manager User Guide*.

For more information about Amazon RDS security, see [Security in Amazon RDS \(p. 1997\)](#). For more information about IAM, see [AWS Identity and Access Management](#). For information on IAM best practices, see [IAM best practices](#).

Use the AWS Management Console, the AWS CLI, or the RDS API to change the password for your master user. If you use another tool, such as a SQL client, to change the master user password, it might result in privileges being revoked for the user unintentionally.

Controlling access with security groups

VPC security groups control the access that traffic has in and out of a DB instance. By default, network access is turned off for a DB instance. You can specify rules in a security group that allow access from an IP address range, port, or security group. After ingress rules are configured, the same rules apply to all DB instances that are associated with that security group. You can specify up to 20 rules in a security group.

Overview of VPC security groups

Each VPC security group rule makes it possible for a specific source to access a DB instance in a VPC that is associated with that VPC security group. The source can be a range of addresses (for example, 203.0.113.0/24), or another VPC security group. By specifying a VPC security group as the source, you allow incoming traffic from all instances (typically application servers) that use the source VPC security group. VPC security groups can have rules that govern both inbound and outbound traffic. However, the outbound traffic rules typically don't apply to DB instances. Outbound traffic rules apply only if the DB instance acts as a client. For example, outbound traffic rules apply to an Oracle DB instance with outbound database links. You must use the [Amazon EC2 API](#) or the **Security Group** option on the VPC console to create VPC security groups.

When you create rules for your VPC security group that allow access to the instances in your VPC, you must specify a port for each range of addresses that the rule allows access for. For example, if you want to turn on Secure Shell (SSH) access for instances in the VPC, create a rule allowing access to TCP port 22 for the specified range of addresses.

You can configure multiple VPC security groups that allow access to different ports for different instances in your VPC. For example, you can create a VPC security group that allows access to TCP port 80 for web servers in your VPC. You can then create another VPC security group that allows access to TCP port 3306 for RDS for MySQL DB instances in your VPC.

For more information on VPC security groups, see [Security groups](#) in the *Amazon Virtual Private Cloud User Guide*.

Note

If your DB instance is in a VPC but isn't publicly accessible, you can also use an AWS Site-to-Site VPN connection or an AWS Direct Connect connection to access it from a private network. For more information, see [Internetwork traffic privacy \(p. 2015\)](#).

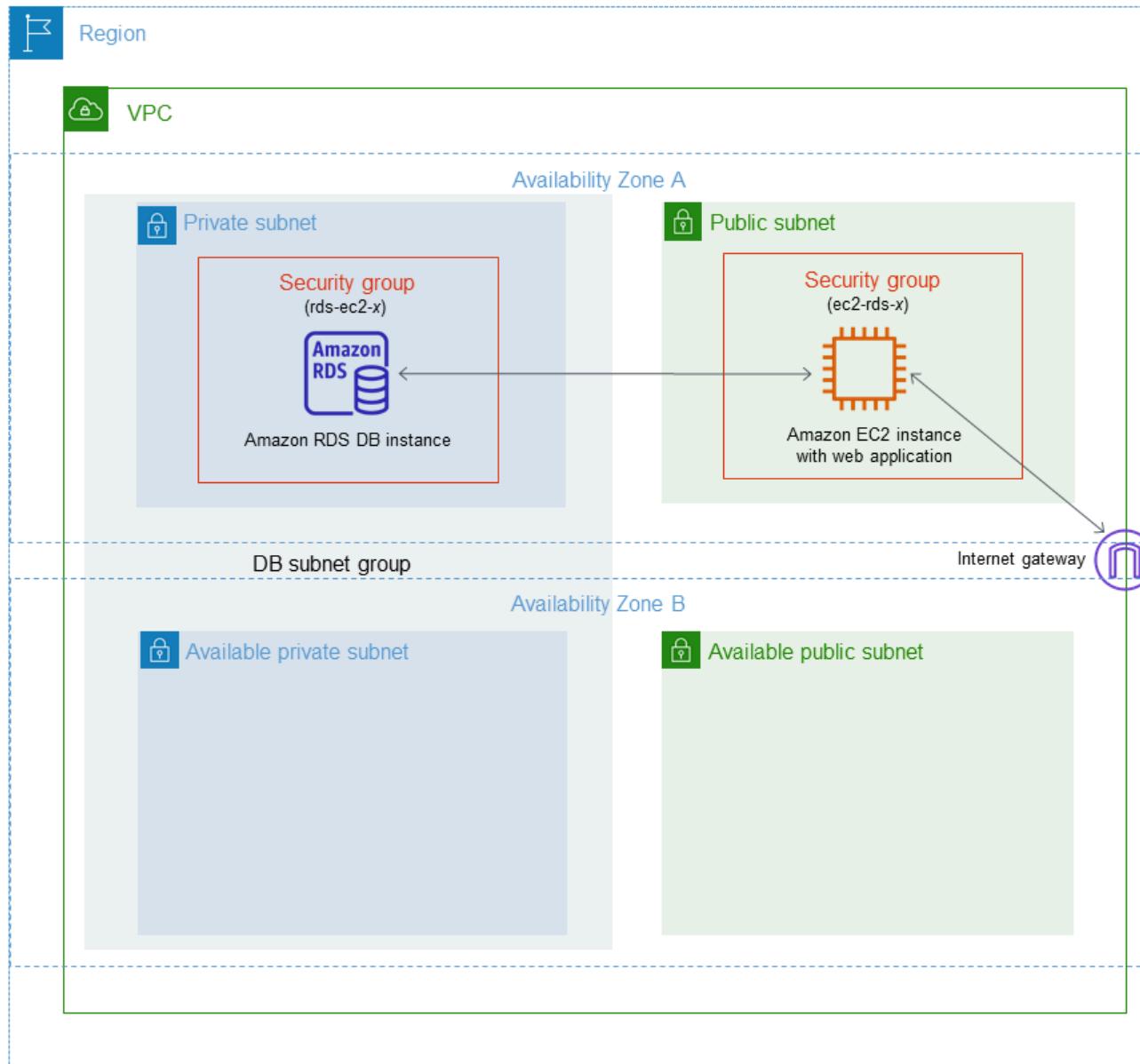
Security group scenario

A common use of a DB instance in a VPC is to share data with an application server running in an Amazon EC2 instance in the same VPC, which is accessed by a client application outside the VPC. For this scenario, you use the RDS and VPC pages on the AWS Management Console or the RDS and EC2 API operations to create the necessary instances and security groups:

1. Create a VPC security group (for example, sg-0123ec2example) and define inbound rules that use the IP addresses of the client application as the source. This security group allows your client application to connect to EC2 instances in a VPC that uses this security group.
2. Create an EC2 instance for the application and add the EC2 instance to the VPC security group (sg-0123ec2example) that you created in the previous step.
3. Create a second VPC security group (for example, sg-6789rdsexample) and create a new rule by specifying the VPC security group that you created in step 1 (sg-0123ec2example) as the source.

4. Create a new DB instance and add the DB instance to the VPC security group (sg-6789rdsexample) that you created in the previous step. When you create the DB instance, use the same port number as the one specified for the VPC security group (sg-6789rdsexample) rule that you created in step 3.

The following diagram shows this scenario.



For detailed instructions about configuring a VPC for this scenario, see [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#). For more information about using a VPC, see [Amazon VPC VPCs](#) and [Amazon RDS \(p. 2103\)](#).

Creating a VPC security group

You can create a VPC security group for a DB instance by using the VPC console. For information about creating a security group, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#) and [Security groups](#) in the *Amazon Virtual Private Cloud User Guide*.

Associating a security group with a DB instance

You can associate a security group with a DB instance by using **Modify** on the RDS console, the `ModifyDBInstance` Amazon RDS API, or the `modify-db-instance` AWS CLI command.

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#). For security group considerations when you restore a DB instance from a DB snapshot, see [Security group considerations \(p. 452\)](#).

Master user account privileges

When you create a new DB instance, the default master user that you use gets certain privileges for that DB instance. You can't change the master user name after the DB instance is created.

Important

We strongly recommend that you do not use the master user directly in your applications. Instead, adhere to the best practice of using a database user created with the minimal privileges required for your application.

Note

If you accidentally delete the permissions for the master user, you can restore them by modifying the DB instance and setting a new master user password. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

The following table shows the privileges and database roles the master user gets for each of the database engines.

Database engine	System privilege	Database role
MySQL and MariaDB	SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION CLIENT, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER ON *.* WITH GRANT OPTION, REPLICATION SLAVE	—
PostgreSQL	CREATE ROLE, CREATE DB, PASSWORD VALID UNTIL INFINITY, CREATE EXTENSION, ALTER EXTENSION, DROP EXTENSION, CREATE TABLESPACE, ALTER <OBJECT> OWNER, CHECKPOINT, PG_CANCEL_BACKEND(), PG_TERMINATE_BACKEND(), SELECT PG_STAT_REPLICATION, EXECUTE PG_STAT_STATEMENTS_RESET(), OWN POSTGRES_FDW_HANDLER(), OWN POSTGRES_FDW_VALIDATOR(), OWN POSTGRES_FDW, EXECUTE PG_BUFFERCACHE_PAGES(), SELECT PG_BUFFERCACHE	RDS_SUPERUSER For more information about RDS_SUPERUSER, see Understanding PostgreSQL roles and permissions (p. 1915) .
Oracle	ALTER DATABASE LINK, ALTER PUBLIC DATABASE LINK, DROP ANY DIRECTORY, EXEMPT ACCESS POLICY, EXEMPT IDENTITY POLICY, GRANT ANY OBJECT PRIVILEGE, RESTRICTED SESSION, EXEMPT REDACTION POLICY	AQ_ADMINISTRATOR_ROLE, AQ_USER_ROLE, CONNECT, CTXAPP, DBA, EXECUTE_CATALOG_ROLE, RECOVERY_CATALOG_OWNER, RESOURCE, SELECT_CATALOG_ROLE

Database engine	System privilege	Database role
Microsoft SQL Server	ADMINISTER BULK OPERATIONS, ALTER ANY CONNECTION, ALTER ANY CREDENTIAL, ALTER ANY EVENT SESSION, ALTER ANY LINKED SERVER, ALTER ANY LOGIN, ALTER ANY SERVER AUDIT, ALTER ANY SERVER ROLE, ALTER SERVER STATE, ALTER TRACE, CONNECT SQL, CREATE ANY DATABASE, VIEW ANY DATABASE, VIEW ANY DEFINITION, VIEW SERVER STATE, ALTER ON ROLE SQLAgentOperatorRole	DB_OWNER (database-level role), PROCESSADMIN (server-level role), SETUPADMIN (server-level role), SQLAgentUserRole (database-level role)

Using service-linked roles for Amazon RDS

Amazon RDS uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to Amazon RDS. Service-linked roles are predefined by Amazon RDS and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes using Amazon RDS easier because you don't have to manually add the necessary permissions. Amazon RDS defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon RDS can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete the roles only after first deleting their related resources. This protects your Amazon RDS resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [AWS services that work with IAM](#) and look for the services that have Yes in the **Service-Linked Role** column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for Amazon RDS

Amazon RDS uses the service-linked role named AWSServiceRoleForRDS to allow Amazon RDS to call AWS services on behalf of your DB instances.

The AWSServiceRoleForRDS service-linked role trusts the following services to assume the role:

- rds.amazonaws.com

This service-linked role has a permissions policy attached to it called `AmazonRDSServiceRolePolicy` that grants it permissions to operate in your account. The role permissions policy allows Amazon RDS to complete the following actions on the specified resources:

```

    "ec2:DescribeCoipPools",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTablePermissions",
    "ec2:DescribeLocalGatewayRouteTables",
    "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcAttribute",
    "ec2:DescribeVpcs",
    "ec2:DisassociateAddress",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:ModifyVpcEndpoint",
    "ec2:ReleaseAddress",
    "ec2:RevokeSecurityGroupIngress",
    "ec2>CreateVpcEndpoint",
    "ec2:DescribeVpcEndpoints",
    "ec2:DeleteVpcEndpoints",
    "ec2:AssignPrivateIpAddresses",
    "ec2:UnassignPrivateIpAddresses"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "sns:Publish"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
    "logs>CreateLogGroup"
],
"Resource": [
    "arn:aws:logs:***:log-group:/aws/rds/*",
    "arn:aws:logs:***:log-group:/aws/docdb/*",
    "arn:aws:logs:***:log-group:/aws/neptune/*"
]
},
{
"Effect": "Allow",
"Action": [
    "logs>CreateLogStream",
    "logs:PutLogEvents",
    "logs:DescribeLogStreams"
],
"Resource": [
    "arn:aws:logs:***:log-group:/aws/rds/*:log-stream:*",
    "arn:aws:logs:***:log-group:/aws/docdb/*:log-stream:*",
    "arn:aws:logs:***:log-group:/aws/neptune/*:log-stream:*
```

```

        "Resource": [
            "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "cloudwatch:PutMetricData"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "cloudwatch:namespace": [
                    "AWS/DocDB",
                    "AWS/Neptune",
                    "AWS/RDS",
                    "AWS/Usage"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret",
            "secretsmanager:RestoreSecret",
            "secretsmanager>CreateSecret",
            "secretsmanager>DeleteSecret",
            "secretsmanager:UpdateSecret"
        ],
        "Resource": "arn:aws:secretsmanager:*:*:secret:rds-sqlserver-ssrs!*"
    }
}
]
}

```

Note

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. If you encounter the following error message:

Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.

Make sure you have the following permissions enabled:

```

{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "rds.amazonaws.com"
        }
    }
}

```

For more information, see [Service-linked role permissions in the *IAM User Guide*](#).

Creating a service-linked role for Amazon RDS

You don't need to manually create a service-linked role. When you create a DB instance, Amazon RDS creates the service-linked role for you.

Important

If you were using the Amazon RDS service before December 1, 2017, when it began supporting service-linked roles, then Amazon RDS created the AWSServiceRoleForRDS role in your account. To learn more, see [A new role appeared in my AWS account](#).

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a DB instance, Amazon RDS creates the service-linked role for you again.

Editing a service-linked role for Amazon RDS

Amazon RDS does not allow you to edit the AWSServiceRoleForRDS service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a service-linked role](#) in the *IAM User Guide*.

Deleting a service-linked role for Amazon RDS

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must delete all of your DB instances before you can delete the service-linked role.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role.

To check whether the service-linked role has an active session in the IAM console

1. Sign in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
2. In the navigation pane of the IAM console, choose **Roles**. Then choose the name (not the check box) of the AWSServiceRoleForRDS role.
3. On the **Summary** page for the chosen role, choose the **Access Advisor** tab.
4. On the **Access Advisor** tab, review recent activity for the service-linked role.

Note

If you are unsure whether Amazon RDS is using the AWSServiceRoleForRDS role, you can try to delete the role. If the service is using the role, then the deletion fails and you can view the AWS Regions where the role is being used. If the role is being used, then you must wait for the session to end before you can delete the role. You cannot revoke the session for a service-linked role.

If you want to remove the AWSServiceRoleForRDS role, you must first delete *all* of your DB instances .

Deleting all of your instances

Use one of these procedures to delete each of your instances.

To delete an instance (console)

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the instance that you want to delete.
4. For **Actions**, choose **Delete**.

5. If you are prompted for **Create final Snapshot?**, choose Yes or No.
 6. If you chose Yes in the previous step, for **Final snapshot name** enter the name of your final snapshot.
 7. Choose **Delete**.

To delete an instance (CLI)

See [delete-db-instance](#) in the *AWS CLI Command Reference*.

To delete an instance (API)

See [DeleteDBInstance](#) in the *Amazon RDS API Reference*.

You can use the IAM console, the IAM CLI, or the IAM API to delete the AWSServiceRoleForRDS service-linked role. For more information, see [Deleting a service-linked role](#) in the *IAM User Guide*.

Service-linked role permissions for Amazon RDS

Custom

Amazon RDS Custom uses the service-linked role named `AWSServiceRoleForRDSCustom` to allow RDS Custom to call AWS services on behalf of your DB instances and DB clusters.

The AWSServiceRoleForRDSCustom service-linked role trusts the following services to assume the role:

- custom.rds.amazonaws.com

This service-linked role has a permissions policy attached to it called `AmazonRDSCustomServiceRolePolicy` that grants it permissions to operate in your account. The role permissions policy allows RDS Custom to complete the following actions on the specified resources:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "ecc1",  
      "Effect": "Allow",  
      "Action": [  
        "ec2:DescribeInstances",  
        "ec2:DescribeInstanceAttribute",  
        "ec2:DescribeRegions",  
        "ec2:DescribeSnapshots",  
        "ec2:DescribeNetworkInterfaces",  
        "ec2:DescribeVolumes",  
        "ec2:DescribeInstanceStatus",  
        "ec2:DescribeIamInstanceProfileAssociations",  
        "ec2:DescribeImages",  
        "ec2:DescribeVpcs",  
        "ec2:RegisterImage",  
        "ec2:DeregisterImage",  
        "ec2:DescribeTags",  
        "ec2:DescribeSecurityGroups",  
        "ec2:DescribeVolumesModifications",  
        "ec2:DescribeSubnets",  
        "ec2:DescribeVpcAttribute",  
        "ec2:SearchTransitGatewayMulticastGroups",  
        "ec2:GetTransitGatewayMulticastDomainAssociations",  
        "ec2:DescribeTransitGatewayMulticastDomains",  
        "ec2:DescribeTransitGateways".  
      ]  
    }  
  ]  
}
```

```

    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeRouteTables"
],
"Resource": [
    "*"
]
},
{
    "Sid": "ecc2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
    ],
    "Resource": "arn:aws:ec2:*::instance/*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "ecc1scoping",
    "Effect": "Allow",
    "Action": [
        "ec2:AllocateAddress"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "ecc1scoping2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
}
]
```

```

        "custom-oracle-rac"
    ]
}
},
{
    "Sid": "eccRunInstances1",
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
        "arn:aws:ec2:*::instance/*",
        "arn:aws:ec2:*::volume/*",
        "arn:aws:ec2:*::network-interface/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccRunInstances2",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:*::subnet/*",
        "arn:aws:ec2:*::security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*::placement-group/*"
    ]
},
{
    "Sid": "eccRunInstances3",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:*::network-interface/*",
        "arn:aws:ec2::*:snapshot/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "RequireImdsV2",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*::instance/*",
    "Condition": {
        "StringNotEquals": {
            "ec2:MetadataHttpTokens": "required"
        },
        "StringLike": {

```

```
    "aws:RequestTag/AWSRDSCustom": [
        "custom-oracle-rac"
    ]
}
},
{
    "Sid": "eccRunInstances3keyPair1",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
    ],
    "Resource": [
        "arn:aws:ec2:*::*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccKeyPair2",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateKeyPair"
    ],
    "Resource": [
        "arn:aws:ec2:*::*:key-pair/do-not-delete-rds-custom-*"
    ],
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccCreateTag1",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccCreateTag2",

```

```

    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ],
            "ec2:CreateAction": [
                "CreateKeyPair",
                "RunInstances",
                "CreateVolume",
                "CreateSnapshots",
                "CopySnapshot",
                "AllocateAddress"
            ]
        }
    }
},
{
    "Sid": "eccVolume1",
    "Effect": "Allow",
    "Action": [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*.*:instance/*",
        "arn:aws:ec2:*.*:volume/*"
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccVolume2",
    "Effect": "Allow",
    "Action": "ec2>CreateVolume",
    "Resource": "arn:aws:ec2:*.*:volume/*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eccVolume3",
    "Effect": "Allow",
    "Action": [
        "ec2:ModifyVolumeAttribute",
        "ec2>DeleteVolume",
        "ec2:ModifyVolume"
    ],
    "Resource": "arn:aws:ec2:*.*:volume/*",

```

```

    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWSRDSCustom": [
          "custom-oracle",
          "custom-sqlserver",
          "custom-oracle-rac"
        ]
      }
    },
    {
      "Sid": "eccVolume4snapshot1",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:::snapshot/*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AWSRDSCustom": [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid": "eccSnapshot2",
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "arn:aws:ec2:::snapshot/*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AWSRDSCustom": [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid": "eccSnapshot3",
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": [
        "arn:aws:ec2::*:instance/*",
        "arn:aws:ec2::*:volume/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AWSRDSCustom": [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid": "iam1",

```

```

    "Effect": "Allow",
    "Action": [
        "iam:ListInstanceProfiles",
        "iamGetInstanceProfile",
        "iam:GetRole",
        "iam>ListRolePolicies",
        "iam:GetRolePolicy",
        "iam>ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
    ],
    "Resource": "*"
},
{
    "Sid": "iam2",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/AWSRDSCustom*",
    "Condition": {
        "StringLike": {
            "iam:PassedToService": "ec2.amazonaws.com"
        }
    }
},
{
    "Sid": "cloudtrail1",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:GetTrailStatus"
    ],
    "Resource": "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
},
{
    "Sid": "cw1",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch>DeleteAlarms"
    ],
    "Resource": "arn:aws:cloudwatch:::alarm:do-not-delete-rds-custom-*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "cw2",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
    ],
    "Resource": "arn:aws:cloudwatch:::alarm:do-not-delete-rds-custom-*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
}

```

```

        },
        {
          "Sid": "cw3",
          "Effect": "Allow",
          "Action": [
            "cloudwatch:DescribeAlarms"
          ],
          "Resource": "arn:aws:cloudwatch:*:*:alarm:*
        },
        {
          "Sid": "ssm1",
          "Effect": "Allow",
          "Action": "ssm:SendCommand",
          "Resource": "arn:aws:ssm:*:*:document/*"
        },
        {
          "Sid": "ssm2",
          "Effect": "Allow",
          "Action": "ssm:SendCommand",
          "Resource": "arn:aws:ec2:*:*:instance/*",
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
              ]
            }
          }
        },
        {
          "Sid": "ssm3",
          "Effect": "Allow",
          "Action": [
            "ssm:GetCommandInvocation",
            "ssm:GetConnectionStatus",
            "ssm:DescribeInstanceInformation"
          ],
          "Resource": "*"
        },
        {
          "Sid": "ssm4",
          "Effect": "Allow",
          "Action": [
            "ssm:PutParameter",
            "ssm:AddTagsToResource"
          ],
          "Resource": "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
          "Condition": {
            "StringLike": {
              "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle-rac"
              ]
            }
          }
        },
        {
          "Sid": "ssm5",
          "Effect": "Allow",
          "Action": [
            "ssm:DeleteParameter"
          ],
          "Resource": "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
          "Condition": {
            "StringLike": {

```

```
    "aws:ResourceTag/AWSRDSCustom": [
        "custom-oracle-rac"
    ]
}
},
{
    "Sid": "eb1",
    "Effect": "Allow",
    "Action": [
        "events:PutRule",
        "events:TagResource"
    ],
    "Resource": "arn:aws:events:*::rule/do-not-delete-rds-custom-*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "eb2",
    "Effect": "Allow",
    "Action": [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events>ListTargetsByRule",
        "events>DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
    ],
    "Resource": "arn:aws:events:*::rule/do-not-delete-rds-custom-*",
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
{
    "Sid": "secretmanager1",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:TagResource",
        "secretsmanager>CreateSecret"
    ],
    "Resource": "arn:aws:secretsmanager:*::secret:do-not-delete-rds-custom-*",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/AWSRDSCustom": [
                "custom-oracle",
                "custom-sqlserver",
                "custom-oracle-rac"
            ]
        }
    }
},
```

```
"Sid": "secretmanager2",
"Effect": "Allow",
>Action": [
    "secretsmanager:TagResource",
    "secretsmanager:DescribeSecret",
    "secretsmanager>DeleteSecret",
    "secretsmanager:PutSecretValue"
],
"Resource": "arn:aws:secretsmanager:*::secret:do-not-delete-rds-custom-*",
"Condition": {
    "StringLike": {
        "aws:ResourceTag/AWSRDSCustom": [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
        ]
    }
}
]
```

Creating, editing, or deleting the service-linked role for RDS Custom works the same as for Amazon RDS. For more information, see [Service-linked role permissions for Amazon RDS \(p. 2089\)](#).

Note

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. If you encounter the following error message:

Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.

Make sure you have the following permissions enabled:

```
{
    "Action": "iam>CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/custom.rds.amazonaws.com/
AmazonRDSCustomServiceRolePolicy",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "custom.rds.amazonaws.com"
        }
    }
}
```

For more information, see [Service-linked role permissions in the IAM User Guide](#).

Amazon VPC VPCs and Amazon RDS

Amazon Virtual Private Cloud (Amazon VPC) makes it possible for you to launch AWS resources, such as Amazon RDS DB instances, into a virtual private cloud (VPC).

When you use a VPC, you have control over your virtual networking environment. You can choose your own IP address range, create subnets, and configure routing and access control lists. There is no additional cost to run your DB instance in a VPC.

Accounts have a default VPC. All new DB instances are created in the default VPC unless you specify otherwise.

Topics

- [Working with a DB instance in a VPC \(p. 2103\)](#)
- [Updating the VPC for a DB instance \(p. 2114\)](#)
- [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#)
- [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#)
- [Tutorial: Create a VPC for use with a DB instance \(dual-stack mode\) \(p. 2126\)](#)
- [Moving a DB instance not in a VPC into a VPC \(p. 2133\)](#)

Following, you can find a discussion about VPC functionality relevant to Amazon RDS DB instances. For more information about Amazon VPC, see [Amazon VPC Getting Started Guide](#) and [Amazon VPC User Guide](#).

Working with a DB instance in a VPC

Your DB instance is in a virtual private cloud (VPC). A VPC is a virtual network that is logically isolated from other virtual networks in the AWS Cloud. Amazon VPC makes it possible for you to launch AWS resources, such as an Amazon RDS DB instance or Amazon EC2 instance, into a VPC. The VPC can either be a default VPC that comes with your account or one that you create. All VPCs are associated with your AWS account.

Your default VPC has three subnets that you can use to isolate resources inside the VPC. The default VPC also has an internet gateway that can be used to provide access to resources inside the VPC from outside the VPC.

For a list of scenarios involving Amazon RDS DB instances in a VPC and outside of a VPC, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

Topics

- [Working with a DB instance in a VPC \(p. 2104\)](#)
- [Working with DB subnet groups \(p. 2104\)](#)
- [Amazon RDS IP addressing \(p. 2105\)](#)
- [Hiding a DB instance in a VPC from the internet \(p. 2109\)](#)
- [Creating a DB instance in a VPC \(p. 2111\)](#)

In the following tutorials, you can learn to create a VPC that you can use for a common Amazon RDS scenario:

- [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#)
- [Tutorial: Create a VPC for use with a DB instance \(dual-stack mode\) \(p. 2126\)](#)

Working with a DB instance in a VPC

Here are some tips on working with a DB instance in a VPC:

- Your VPC must have at least two subnets. These subnets must be in two different Availability Zones in the AWS Region where you want to deploy your DB instance. A *subnet* is a segment of a VPC's IP address range that you can specify and that you can use to group DB instances based on your security and operational needs.

For Multi-AZ deployments, defining a subnet for two or more Availability Zones in an AWS Region allows Amazon RDS to create a new standby in another Availability Zone as needed. Make sure to do this even for Single-AZ deployments, just in case you want to convert them to Multi-AZ deployments at some point.

Note

The DB subnet group for a Local Zone can have only one subnet.

- If you want your DB instance in the VPC to be publicly accessible, make sure to turn on the VPC attributes *DNS hostnames* and *DNS resolution*.
- Your VPC must have a DB subnet group that you create. You create a DB subnet group by specifying the subnets you created. Amazon RDS chooses a subnet and an IP address within that subnet to associate with your DB instance. The DB instance uses the Availability Zone that contains the subnet.
- Your VPC must have a VPC security group that allows access to the DB instance.

For more information, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

- The CIDR blocks in each of your subnets must be large enough to accommodate spare IP addresses for Amazon RDS to use during maintenance activities, including failover and compute scaling. For example, a range such as 10.0.0.0/24 and 10.0.1.0/24 is typically large enough.
- A VPC can have an *instance tenancy* attribute of either *default* or *dedicated*. All default VPCs have the instance tenancy attribute set to default, and a default VPC can support any DB instance class.

If you choose to have your DB instance in a dedicated VPC where the instance tenancy attribute is set to dedicated, the DB instance class of your DB instance must be one of the approved Amazon EC2 dedicated instance types. For example, the r5.large EC2 dedicated instance corresponds to the db.r5.large DB instance class. For information about instance tenancy in a VPC, see [Dedicated instances](#) in the [Amazon Elastic Compute Cloud User Guide](#).

For more information about the instance types that can be in a dedicated instance, see [Amazon EC2 dedicated instances](#) on the EC2 pricing page.

Note

When you set the instance tenancy attribute to dedicated for a DB instance, it doesn't guarantee that the DB instance will run on a dedicated host.

- When an option group is assigned to a DB instance, it's associated with the DB instance's VPC. This linkage means that you can't use the option group assigned to a DB instance if you attempt to restore the DB instance into a different VPC.
- If you restore a DB instance into a different VPC, make sure to either assign the default option group to the DB instance, assign an option group that is linked to that VPC, or create a new option group and assign it to the DB instance. With persistent or permanent options, such as Oracle TDE, you must create a new option group that includes the persistent or permanent option when restoring a DB instance into a different VPC.

Working with DB subnet groups

Subnets are segments of a VPC's IP address range that you designate to group your resources based on security and operational needs. A *DB subnet group* is a collection of subnets (typically private) that you

create in a VPC and that you then designate for your DB instances. By using a DB subnet group, you can specify a particular VPC when creating DB instances using the AWS CLI or RDS API. If you use the console, you can choose the VPC and subnet groups you want to use.

Each DB subnet group should have subnets in at least two Availability Zones in a given AWS Region. When creating a DB instance in a VPC, you choose a DB subnet group for it. From the DB subnet group, Amazon RDS chooses a subnet and an IP address within that subnet to associate with the DB instance. The DB uses the Availability Zone that contains the subnet.

If the primary DB instance of a Multi-AZ deployment fails, Amazon RDS can promote the corresponding standby and later create a new standby using an IP address of the subnet in one of the other Availability Zones.

The subnets in a DB subnet group are either public or private. The subnets are public or private, depending on the configuration that you set for their network access control lists (network ACLs) and routing tables. For a DB instance to be publicly accessible, all of the subnets in its DB subnet group must be public. If a subnet that's associated with a publicly accessible DB instance changes from public to private, it can affect DB instance availability.

To create a DB subnet group that supports dual-stack mode, make sure that each subnet that you add to the DB subnet group has an Internet Protocol version 6 (IPv6) CIDR block associated with it. For more information, see [Amazon RDS IP addressing \(p. 2105\)](#) and [Migrating to IPv6](#) in the *Amazon VPC User Guide*.

Note

The DB subnet group for a Local Zone can have only one subnet.

When Amazon RDS creates a DB instance in a VPC, it assigns a network interface to your DB instance by using an IP address from your DB subnet group. However, we strongly recommend that you use the Domain Name System (DNS) name to connect to your DB instance. We recommend this because the underlying IP address changes during failover.

Note

For each DB instance that you run in a VPC, make sure to reserve at least one address in each subnet in the DB subnet group for use by Amazon RDS for recovery actions.

Amazon RDS IP addressing

IP addresses enable resources in your VPC to communicate with each other, and with resources over the internet. Amazon RDS support both the Internet Protocol version 4 (IPv4) and IPv6 addressing protocols. By default, Amazon RDS and Amazon VPC use the IPv4 addressing protocol. You can't turn off this behavior. When you create a VPC, make sure to specify an IPv4 CIDR block (a range of private IPv4 addresses). You can optionally assign an IPv6 CIDR block to your VPC and subnets, and assign IPv6 addresses from that block to DB instances in your subnet.

Support for the IPv6 protocol expands the number of supported IP addresses. By using the IPv6 protocol, you ensure that you have sufficient available addresses for the future growth of the internet. New and existing RDS resources can use IPv4 and IPv6 addresses within your Amazon VPC. Configuring, securing, and translating network traffic between the two protocols used in different parts of an application can cause operational overhead. You can standardize on the IPv6 protocol for Amazon RDS resources to simplify your network configuration.

Topics

- [IPv4 addresses \(p. 2106\)](#)
- [IPv6 addresses \(p. 2106\)](#)
- [Dual-stack mode \(p. 2106\)](#)

IPv4 addresses

When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a CIDR block, such as `10.0.0.0/16`. A *DB subnet group* defines the range of IP addresses in this CIDR block that a DB instance can use. These IP addresses can be private or public.

A private IPv4 address is an IP address that's not reachable over the internet. You can use private IPv4 addresses for communication between your DB instance and other resources, such as Amazon EC2 instances, in the same VPC. Each DB instance has a private IP address for communication in the VPC.

A public IP address is an IPv4 address that's reachable from the internet. You can use public addresses for communication between your DB instance and resources on the internet, such as a SQL client. You control whether your DB instance receives a public IP address.

For a tutorial that shows you how to create a VPC with only private IPv4 addresses that you can use for a common Amazon RDS scenario, see [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).

IPv6 addresses

You can optionally associate an IPv6 CIDR block with your VPC and subnets, and assign IPv6 addresses from that block to the resources in your VPC. Each IPv6 address is globally unique.

The IPv6 CIDR block for your VPC is automatically assigned from Amazon's pool of IPv6 addresses. You can't choose the range yourself.

When connecting to an IPv6 address, make sure that the following conditions are met:

- The client is configured so that client to database traffic over IPv6 is allowed.
- RDS security groups used by the DB instance are configured correctly so that client to database traffic over IPv6 is allowed.
- The client operating system stack allows traffic on the IPv6 address, and operating system drivers and libraries are configured to choose the correct default DB instance endpoint (either IPv4 or IPv6).

For more information about IPv6, see [IP Addressing in the Amazon VPC User Guide](#).

Dual-stack mode

When a DB instance can communicate over both the IPv4 and IPv6 addressing protocols, it's running in dual-stack mode. So, resources can communicate with the DB instance over IPv4, IPv6, or both. RDS disables Internet Gateway access for IPv6 endpoints of private dual-stack mode DB instances. RDS does this to ensure that your IPv6 endpoints are private and can only be accessed from within your VPC.

Topics

- [Dual-stack mode and DB subnet groups \(p. 2107\)](#)
- [Working with dual-stack mode DB instances \(p. 2107\)](#)
- [Modifying IPv4-only DB instances to use dual-stack mode \(p. 2107\)](#)
- [Region and version availability \(p. 2109\)](#)
- [Limitations for dual-stack network DB instances \(p. 2109\)](#)

For a tutorial that shows you how to create a VPC with both IPv4 and IPv6 addresses that you can use for a common Amazon RDS scenario, see [Tutorial: Create a VPC for use with a DB instance \(dual-stack mode\) \(p. 2126\)](#).

Dual-stack mode and DB subnet groups

To use dual-stack mode, make sure that each subnet in the DB subnet group that you associate with the DB instance has an IPv6 CIDR block associated with it. You can create a new DB subnet group or modify an existing DB subnet group to meet this requirement. After a DB instance is in dual-stack mode, clients can connect to it normally. Make sure that client security firewalls and RDS DB instance security groups are accurately configured to allow traffic over IPv6. To connect, clients use the DB instance's endpoint. Client applications can specify which protocol is preferred when connecting to a database. In dual-stack mode, the DB instance detects the client's preferred network protocol, either IPv4 or IPv6, and uses that protocol for the connection.

If a DB subnet group stops supporting dual-stack mode because of subnet deletion or CIDR disassociation, there's a risk of an incompatible network state for DB instances that are associated with the DB subnet group. Also, you can't use the DB subnet group when you create new dual-stack mode DB instances.

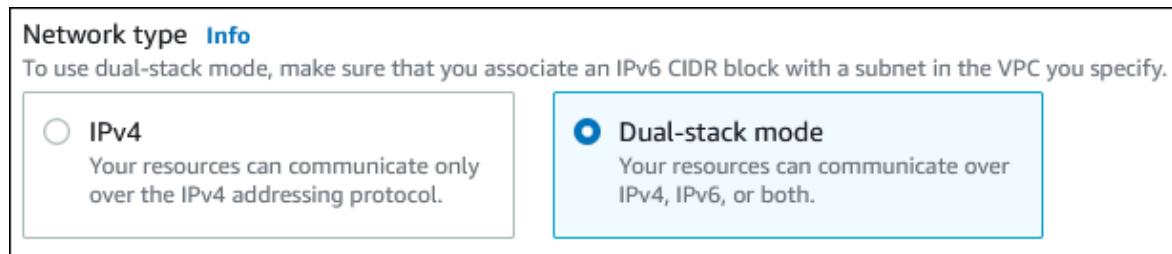
To determine whether a DB subnet group supports dual-stack mode by using the AWS Management Console, view the **Network type** on the details page of the DB subnet group. To determine whether a DB subnet group supports dual-stack mode by using the AWS CLI, call the `describe-db-subnet-groups` command and view `SupportedNetworkTypes` in the output.

Read replicas are treated as independent DB instances and can have a network type that's different from the primary DB instance. If you change the network type of a read replica's primary DB instance, the read replica isn't affected. When you are restoring a DB instance, you can restore it to any network type that's supported.

Working with dual-stack mode DB instances

When you create or modify a DB instance, you can specify *dual-stack mode* to allow your resources to communicate with your DB instance over IPv4, IPv6, or both.

When you use the AWS Management Console to create or modify a DB instance, you can specify dual-stack mode in the **Network type** section. The following image shows the **Network type** section in the console.



When you use the AWS CLI to create or modify a DB instance, set the `--network-type` option to `DUAL` to use dual-stack mode. When you use the RDS API to create or modify a DB instance, set the `NetworkType` parameter to `DUAL` to use dual-stack mode. When you are modifying the network type of a DB instance, downtime is possible. If dual-stack mode isn't supported by the specified DB engine version or DB subnet group, the `NetworkTypeNotSupported` error is returned.

For more information about creating a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#). For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

To determine whether a DB instance is in dual-stack mode by using the console, view the **Network type** on the **Connectivity & security** tab for the DB instance.

Modifying IPv4-only DB instances to use dual-stack mode

You can modify an IPv4-only DB instance to use dual-stack mode. To do so, change the network type of the DB instance. The modification might result in downtime.

Before modifying a DB instance to use dual-stack mode, make sure that its DB subnet group supports dual-stack mode. If the DB subnet group associated with the DB instance doesn't support dual-stack mode, specify a different DB subnet group that supports it when you modify the DB instance. If you modify the DB subnet group of a DB instance before you change the DB instance to use dual-stack mode, make sure that the DB subnet group is valid for the DB instance before and after the change.

If you can't connect to the DB instance after the change, make sure that the client and database security firewalls and route tables are accurately configured to allow cross traffic to the database on the selected network (either IPv4 or IPv6). You might also need to modify operating system parameter, libraries, or drivers to connect using an IPv6 address.

The following limitations apply to modifying a DB instance to use dual-stack mode:

- Dual-stack mode DB instances can't be publicly accessible.
- DB instances can't have an IPv6-only endpoint.
- There can't be a pending change from a Single-AZ deployment to a Multi-AZ deployment, or from a Multi-AZ deployment to a Single-AZ deployment.

To modify an IPv4-only DB instance to use dual-stack mode

1. Modify a DB subnet group to support dual-stack mode, or create a DB subnet group that supports dual-stack mode:

- a. Associate an IPv6 CIDR block with your VPC.

For instructions, see [Associate an IPv6 CIDR block with your VPC](#) in the *Amazon VPC User Guide*.

- b. Attach the IPv6 CIDR block to all of the subnets in your the DB subnet group.

For instructions, see [Associate an IPv6 CIDR block with your subnet](#) in the *Amazon VPC User Guide*.

- c. Confirm that the DB subnet group supports dual-stack mode.

If you are using the AWS Management Console, select the DB subnet group, and make sure that the **Supported network types** value is **Dual, IPv4**.

If you are using the AWS CLI, call the `describe-db-subnet-groups` command, and make sure that the `SupportedNetworkType` value for the DB instance is `Dual, IPv4`.

2. Modify the security group associated with the DB instance to allow IPv6 connections to the database, or create a new security group that allows IPv6 connections.

For instructions, see [Security group rules](#) in the *Amazon VPC User Guide*.

3. Modify the DB instance to support dual-stack mode. To do so, set the **Network type** to **Dual-stack mode**.

If you are using the console, make sure that the following settings are correct:

- **Network type – Dual-stack mode**

Network type [Info](#)

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.



IPv4

Your resources can communicate only over the IPv4 addressing protocol.



Dual-stack mode

Your resources can communicate over IPv4, IPv6, or both.

- **DB subnet group** – The DB subnet group that you configured in a previous step

- **Security group** – The security that you configured in a previous step

If you are using the AWS CLI, make sure that the following settings are correct:

- `--network-type` – dual
 - `--db-subnet-group-name` – The DB subnet group that you configured in a previous step
 - `--vpc-security-group-ids` – The VPC security group that you configured in a previous step
4. Confirm that the DB instance supports dual-stack mode.

If you are using the console, choose the **Connectivity & security** tab for the DB instance. On that tab, make sure that the **Network type** value is **Dual-stack mode**.

If you are using the AWS CLI, call the [describe-db-instances](#) command, and make sure that the `NetworkType` value for the DB instance is dual.

Run the `dig` command on the DB instance endpoint to identify the IPv6 address associated with it.

```
dig db-instance-endpoint AAAA
```

Use the DB instance endpoint, not the IPv6 address, to connect to the DB instance.

Region and version availability

Feature availability and support varies across specific versions of each database engine, and across AWS Regions. For more information on version and Region availability with dual stack mode, see [Dual-stack mode \(p. 88\)](#).

Limitations for dual-stack network DB instances

The following limitations apply to dual-stack network DB instances:

- DB instances can't use the IPv6 protocol exclusively. They can use IPv4 exclusively, or they can use the IPv4 and IPv6 protocol (dual-stack mode).
- Amazon RDS doesn't support native IPv6 subnets.
- DB instances that use dual-stack mode must be private. They can't be publicly accessible.
- Dual-stack mode doesn't support the db.m3 and db.r3 DB instance classes.
- For RDS for SQL Server, dual-stack mode DB instances that use Always On AGs availability group listener endpoints only present IPv4 addresses.
- You can't use RDS Proxy with dual-stack mode DB instances.
- You can't use dual-stack mode with RDS on AWS Outposts DB instances.
- You can't use dual-stack mode with DB instances in a Local Zone.

Hiding a DB instance in a VPC from the internet

One common Amazon RDS scenario is to have a VPC in which you have an EC2 instance with a public-facing web application and a DB instance with a database that isn't publicly accessible. For example, you can create a VPC that has a public subnet and a private subnet. Amazon EC2 instances that function as web servers can be deployed in the public subnet. The DB instances are deployed in the private subnet. In such a deployment, only the web servers have access to the DB instances. For an illustration of this scenario, see [A DB instance in a VPC accessed by an EC2 instance in the same VPC \(p. 2115\)](#).

When you launch a DB instance inside a VPC, the DB instance has a private IP address for traffic inside the VPC. This private IP address isn't publicly accessible. You can use the **Public access** option to

designate whether the DB instance also has a public IP address in addition to the private IP address. If the DB instance is designated as publicly accessible, its DNS endpoint resolves to the private IP address from within the VPC. It resolves to the public IP address from outside of the VPC. Access to the DB instance is ultimately controlled by the security group it uses. That public access is not permitted if the security group assigned to the DB instance doesn't include inbound rules that permit it. In addition, for a DB instance to be publicly accessible, the subnets in its DB subnet group must have an internet gateway. For more information, see [Can't connect to Amazon RDS DB instance \(p. 2141\)](#)

You can modify a DB instance to turn on or off public accessibility by modifying the **Public access** option. The following illustration shows the **Public access** option in the **Additional connectivity configuration** section. To set the option, open the **Additional connectivity configuration** section in the **Connectivity** section.

The screenshot shows the 'Connectivity' configuration page for an Amazon RDS DB instance. The 'Public access' section is highlighted with a red border. The 'Public access' section contains two options: 'Yes' and 'No'. The 'No' option is selected, which is highlighted with a blue border. A note below the 'No' option states: 'Amazon RDS will not assign a public IP address to the DB cluster. Only Amazon EC2 instances and devices inside the VPC can connect to your DB cluster.' Other sections visible include 'Virtual private cloud (VPC)', 'Subnet group', 'VPC security group', and 'Additional configuration'.

Connectivity

Virtual private cloud (VPC) Info
VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-2aed394c) ▾
Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

Subnet group Info
DB subnet group that defines which subnets and IP ranges the DB cluster can use in the VPC you selected.

default ▾

Public access Info

Yes
Amazon EC2 instances and devices outside the VPC can connect to your DB cluster. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the DB cluster.

No
Amazon RDS will not assign a public IP address to the DB cluster. Only Amazon EC2 instances and devices inside the VPC can connect to your DB cluster.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing
Choose existing VPC security groups

Create new
Create new VPC security group

Existing VPC security groups

Choose VPC security groups ▾
default X

▶ Additional configuration

For information about modifying a DB instance to set the **Public access** option, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Creating a DB instance in a VPC

The following procedures help you create a DB instance in a VPC. To use the default VPC, you can begin with step 2, and use the VPC and DB subnet group have already been created for you. If you want to create an additional VPC, you can create a new VPC.

Note

If you want your DB instance in the VPC to be publicly accessible, you must update the DNS information for the VPC by enabling the VPC attributes *DNS hostnames* and *DNS resolution*. For information about updating the DNS information for a VPC instance, see [Updating DNS support for your VPC](#).

Follow these steps to create a DB instance in a VPC:

- [Step 1: Create a VPC \(p. 2111\)](#)
- [Step 2: Create a DB subnet group \(p. 2111\)](#)
- [Step 3: Create a VPC security group \(p. 2114\)](#)
- [Step 4: Create a DB instance in the VPC \(p. 2114\)](#)

Step 1: Create a VPC

Create a VPC with subnets in at least two Availability Zones. You use these subnets when you create a DB subnet group. If you have a default VPC, a subnet is automatically created for you in each Availability Zone in the AWS Region.

For more information, see [Create a VPC with private and public subnets \(p. 2121\)](#), or see [Create a VPC](#) in the *Amazon VPC User Guide*.

Step 2: Create a DB subnet group

A DB subnet group is a collection of subnets (typically private) that you create for a VPC and that you then designate for your DB instances. A DB subnet group allows you to specify a particular VPC when you create DB instances using the AWS CLI or RDS API. If you use the console, you can just choose the VPC and subnets you want to use. Each DB subnet group must have at least one subnet in at least two Availability Zones in the AWS Region. As a best practice, each DB subnet group should have at least one subnet for every Availability Zone in the AWS Region.

For Multi-AZ deployments, defining a subnet for all Availability Zones in an AWS Region enables Amazon RDS to create a new standby replica in another Availability Zone if necessary. You can follow this best practice even for Single-AZ deployments, because you might convert them to Multi-AZ deployments in the future.

For a DB instance to be publicly accessible, the subnets in the DB subnet group must have an internet gateway. For more information about internet gateways for subnets, see [Connect to the internet using an internet gateway](#) in the *Amazon VPC User Guide*.

Note

The DB subnet group for a Local Zone can have only one subnet.

When you create a DB instance in a VPC, you can choose a DB subnet group. Amazon RDS chooses a subnet and an IP address within that subnet to associate with your DB instance. If no DB subnet groups exist, Amazon RDS creates a default subnet group when you create a DB instance. Amazon RDS creates and associates an Elastic Network Interface to your DB instance with that IP address. The DB instance uses the Availability Zone that contains the subnet.

For Multi-AZ deployments, defining a subnet for two or more Availability Zones in an AWS Region allows Amazon RDS to create a new standby in another Availability Zone should the need arise. You need to do

this even For Single-AZ deployments, just in case you want to convert them to Multi-AZ deployments at some point.

In this step, you create a DB subnet group and add the subnets that you created for your VPC.

To create a DB subnet group

1. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Subnet groups**.
3. Choose **Create DB Subnet Group**.
4. For **Name**, type the name of your DB subnet group.
5. For **Description**, type a description for your DB subnet group.
6. For **VPC**, choose the default VPC or the VPC that you created.
7. In the **Add subnets** section, choose the Availability Zones that include the subnets from **Availability Zones**, and then choose the subnets from **Subnets**.

Create DB Subnet Group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name

You won't be able to modify the name after your subnet group has been created.

mydbsubnetgroup

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Description

My DB Subnet Group

VPC

Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

tutorial-vpc (vpc-068fe388385afc014)

Add subnets

Availability Zones

Choose the Availability Zones that include the subnets you want to add.

Choose an availability zone

us-east-1a X us-east-1c X

Subnets

Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

Select subnets

subnet-079bd4b8953aee1dd (10.0.0.0/24) X

subnet-057e85b72c46fdd9a (10.0.1.0/24) X

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
us-east-1a	subnet-079bd4b8953aee1dd	10.0.0.0/24
us-east-1c	subnet-057e85b72c46fdd9a	10.0.1.0/24

Cancel

Create

Note

If you have enabled a Local Zone, you can choose an Availability Zone group on the [Create DB subnet group](#) page. In this case, choose the **Availability Zone group, Availability Zones, and Subnets**.

8. Choose **Create**.

Your new DB subnet group appears in the DB subnet groups list on the RDS console. You can choose the DB subnet group to see details, including all of the subnets associated with the group, in the details pane at the bottom of the window.

Step 3: Create a VPC security group

Before you create your DB instance, you can create a VPC security group to associate with your DB instance. If you don't create a VPC security group, you can use the default security group when you create a DB instance. For instructions on how to create a security group for your DB instance, see [Create a VPC security group for a private DB instance \(p. 2122\)](#), or see [Control traffic to resources using security groups](#) in the *Amazon VPC User Guide*.

Step 4: Create a DB instance in the VPC

In this step, you create a DB instance and use the VPC name, the DB subnet group, and the VPC security group you created in the previous steps.

Note

If you want your DB instance in the VPC to be publicly accessible, you must enable the VPC attributes *DNS hostnames* and *DNS resolution*. For more information, see [DNS attributes for your VPC](#) in the *Amazon VPC User Guide*.

For details on how to create a DB instance, see [Creating an Amazon RDS DB instance \(p. 230\)](#).

When prompted in the **Connectivity** section, enter the VPC name, the DB subnet group, and the VPC security group.

Updating the VPC for a DB instance

You can use the AWS Management Console to move your DB instance to a different VPC.

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#). In the **Connectivity** section of the modify page, shown following, enter the new DB subnet group for **DB subnet group**. The new subnet group must be a subnet group in a new VPC.

Connectivity

Subnet group

default-vpc-665e7a1f



Security group

List of DB security groups to associate with this DB instance.

You can't change the VPC for a DB instance if the following conditions apply:

- The DB instance is in multiple Availability Zones. You can convert the DB instance to a single Availability Zone, move it to a new VPC, and then convert it back to a Multi-AZ DB instance. For more information, see [Multi-AZ deployments for high availability \(p. 121\)](#).
- The DB instance has one or more read replicas. You can remove the read replicas, move the DB instance to a new VPC, and then add the read replicas again. For more information, see [Working with read replicas \(p. 370\)](#).
- The DB instance is a read replica. You can promote the read replica, and then move the standalone DB instance to a new VPC. For more information, see [Promoting a read replica to be a standalone DB instance \(p. 377\)](#).
- The subnet group in the target VPC doesn't have subnets in the DB instance's the Availability Zone. You can add subnets in the DB instance's Availability Zone to the DB subnet group, and then move the DB instance to the new VPC. For more information, see [Working with DB subnet groups \(p. 2104\)](#).

Scenarios for accessing a DB instance in a VPC

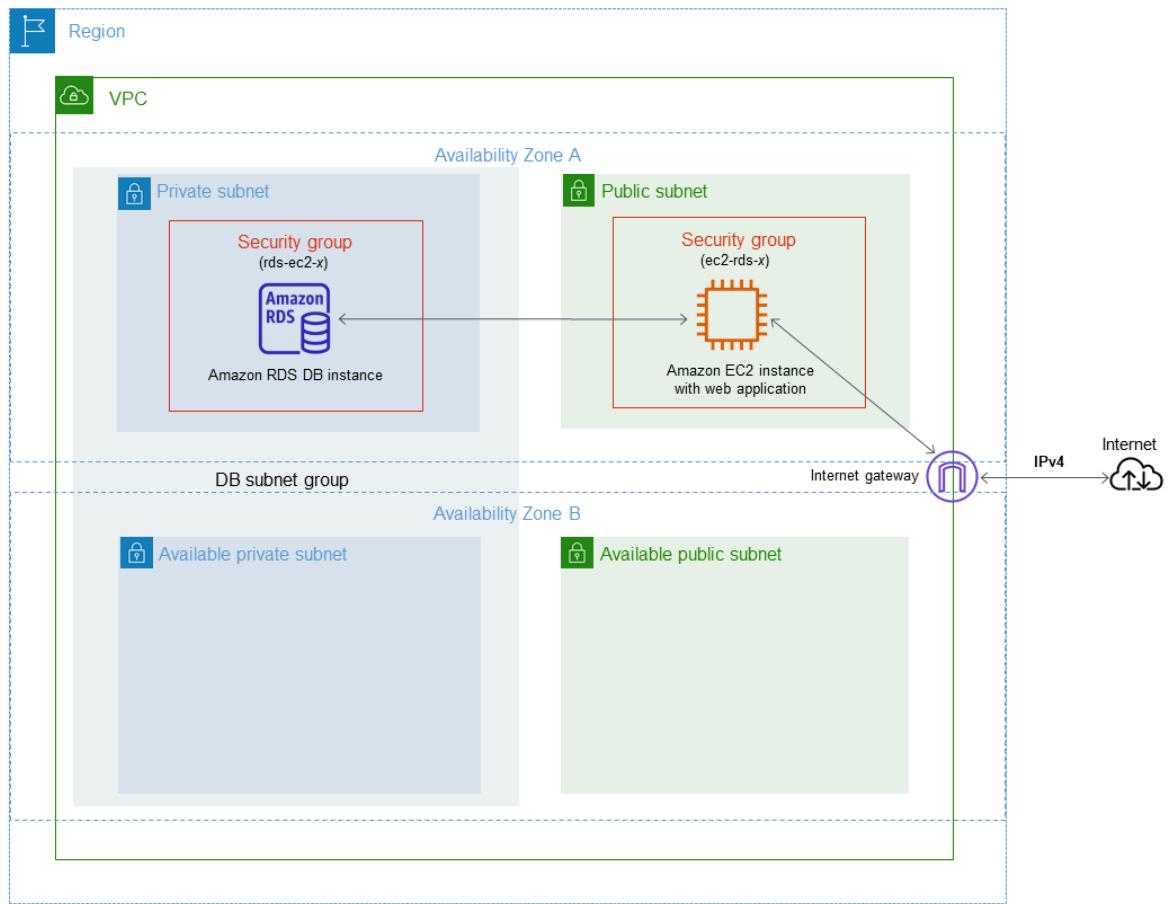
Amazon RDS supports the following scenarios for accessing a DB instance in a VPC:

- [An EC2 instance in the same VPC \(p. 2115\)](#)
- [An EC2 instance in a different VPC \(p. 2117\)](#)
- [A client application through the internet \(p. 2118\)](#)
- [A private network \(p. 2119\)](#)

A DB instance in a VPC accessed by an EC2 instance in the same VPC

A common use of a DB instance in a VPC is to share data with an application server that is running in an EC2 instance in the same VPC.

The following diagram shows this scenario.



The simplest way to manage access between EC2 instances and DB instances in the same VPC is to do the following:

- Create a VPC security group for your DB instances to be in. This security group can be used to restrict access to the DB instances. For example, you can create a custom rule for this security group. This might allow TCP access using the port that you assigned to the DB instance when you created it and an IP address you use to access the DB instance for development or other purposes.
- Create a VPC security group for your EC2 instances (web servers and clients) to be in. This security group can, if needed, allow access to the EC2 instance from the internet by using the VPC's routing table. For example, you can set rules on this security group to allow TCP access to the EC2 instance over port 22.
- Create custom rules in the security group for your DB instances that allow connections from the security group you created for your EC2 instances. These rules might allow any member of the security group to access the DB instances.

There is an additional public and private subnet in a separate Availability Zone. An RDS DB subnet group requires a subnet in at least two Availability Zones. The additional subnet makes it easy to switch to a Multi-AZ DB instance deployment in the future.

For a tutorial that shows you how to create a VPC with both public and private subnets for this scenario, see [Tutorial: Create a VPC for use with a DB instance \(IPv4 only\) \(p. 2120\)](#).

Tip

You can set up network connectivity between an Amazon EC2 instance and a DB instance automatically when you create the DB instance. For more information, see .

To create a rule in a VPC security group that allows connections from another security group, do the following:

1. Sign in to the AWS Management Console and open the Amazon VPC console at <https://console.aws.amazon.com/vpc>.
2. In the navigation pane, choose **Security groups**.
3. Choose or create a security group for which you want to allow access to members of another security group. In the preceding scenario, this is the security group that you use for your DB instances. Choose the **Inbound rules** tab, and then choose **Edit inbound rules**.
4. On the **Edit inbound rules** page, choose **Add rule**.
5. For **Type**, choose the entry that corresponds to the port you used when you created your DB instance, such as **MYSQL/Aurora**.
6. In the **Source** box, start typing the ID of the security group, which lists the matching security groups. Choose the security group with members that you want to have access to the resources protected by this security group. In the scenario preceding, this is the security group that you use for your EC2 instance.
7. If required, repeat the steps for the TCP protocol by creating a rule with **All TCP** as the **Type** and your security group in the **Source** box. If you intend to use the UDP protocol, create a rule with **All UDP** as the **Type** and your security group in **Source**.
8. Choose **Save rules**.

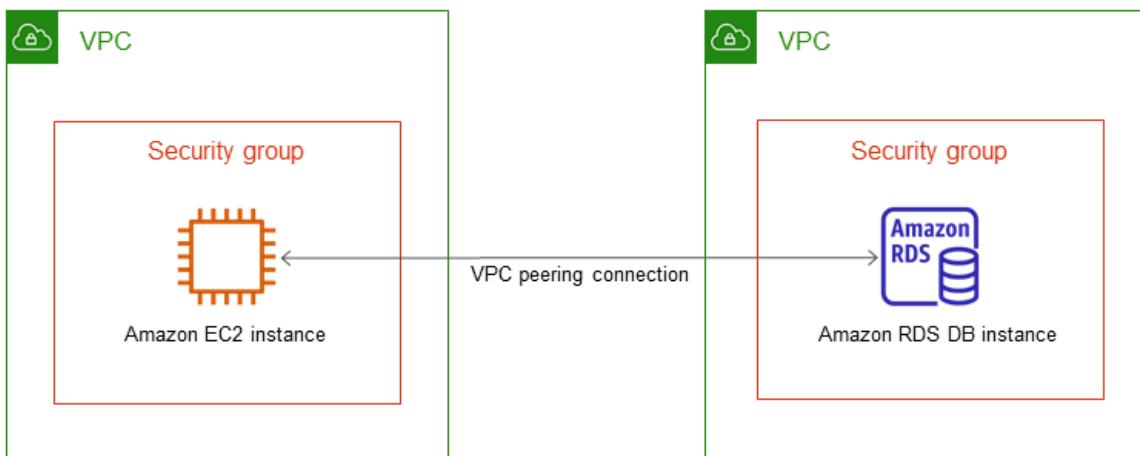
The following screen shows an inbound rule with a security group for its source.

Details	Inbound rules	Outbound rules	Tags
Inbound rules			
Edit inbound rules			
Type	Protocol	Port range	Source
MYSQL/Aurora	TCP	3306	sg-00bd2328e37926844 (tutorial-securitygroup)

A DB instance in a VPC accessed by an EC2 instance in a different VPC

When your DB instances is in a different VPC from the EC2 instance you are using to access it, you can use VPC peering to access the DB instance.

The following diagram shows this scenario.

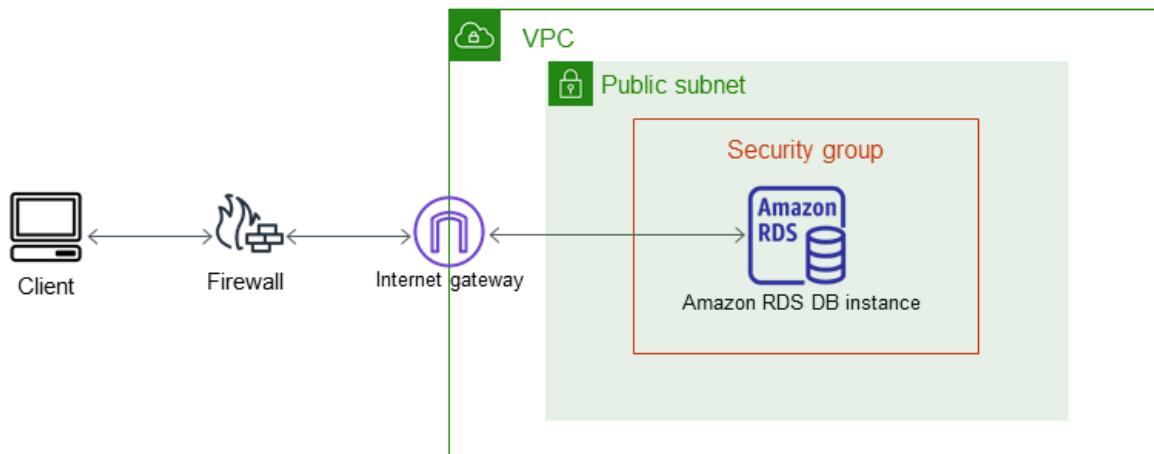


A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IP addresses. Resources in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. To learn more about VPC peering, see [VPC peering](#) in the *Amazon Virtual Private Cloud User Guide*.

A DB instance in a VPC accessed by a client application through the internet

To access a DB instances in a VPC from a client application through the internet, you configure a VPC with a single public subnet, and an internet gateway to enable communication over the internet.

The following diagram shows this scenario.



We recommend the following configuration:

- A VPC of size /16 (for example CIDR: 10.0.0.0/16). This size provides 65,536 private IP addresses.
- A subnet of size /24 (for example CIDR: 10.0.0.0/24). This size provides 256 private IP addresses.
- An Amazon RDS DB instance that is associated with the VPC and the subnet. Amazon RDS assigns an IP address within the subnet to your DB instance.
- An internet gateway which connects the VPC to the internet and to other AWS products.

- A security group associated with the DB instance. The security group's inbound rules allow your client application to access to your DB instance.

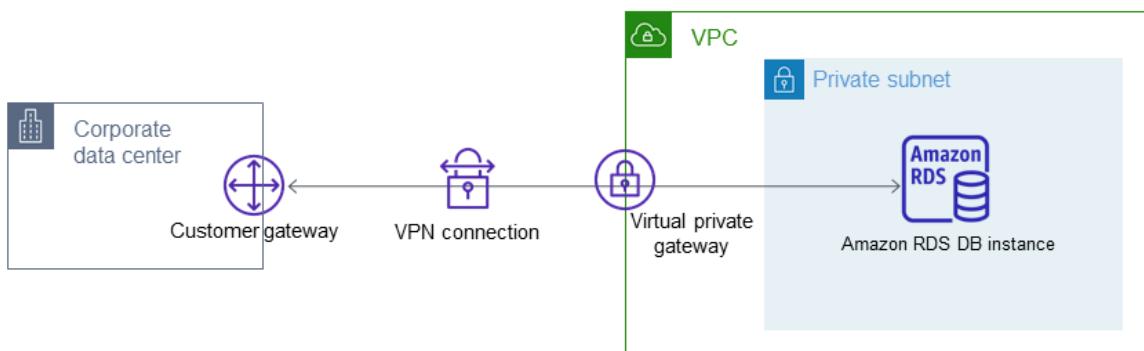
For information about creating a DB instances in a VPC, see [Creating a DB instance in a VPC \(p. 2111\)](#).

A DB instance in a VPC accessed by a private network

If your DB instance isn't publicly accessible, you have the following options for accessing it from a private network:

- An AWS Site-to-Site VPN connection. For more information, see [What is AWS Site-to-Site VPN?](#)
- An AWS Direct Connect connection. For more information, see [What is AWS Direct Connect?](#)

The following diagram shows a scenario with an AWS Site-to-Site VPN connection.

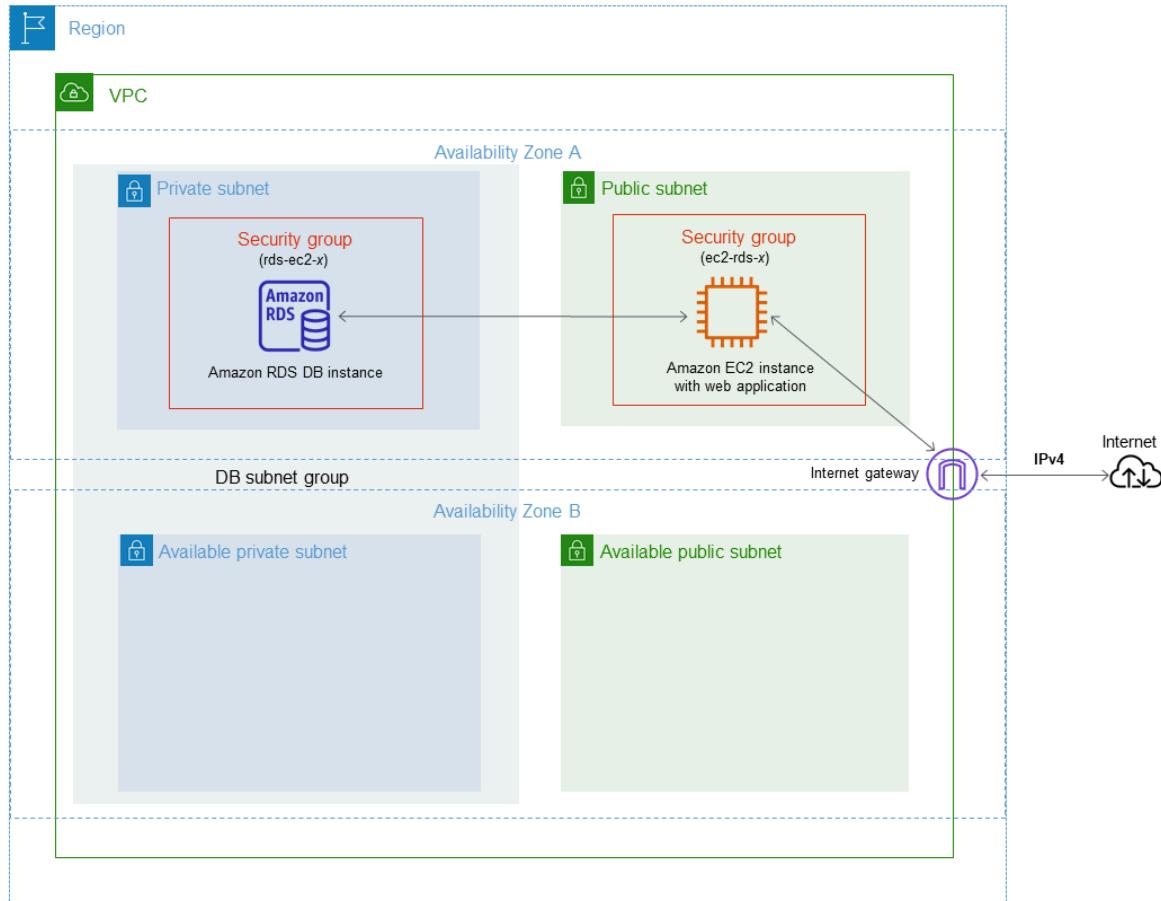


For more information, see [Internetwork traffic privacy \(p. 2015\)](#).

Tutorial: Create a VPC for use with a DB instance (IPv4 only)

A common scenario includes a DB instance in a virtual private cloud (VPC) based on the Amazon VPC service. This VPC shares data with a web server that is running in the same VPC. In this tutorial, you create the VPC for this scenario.

The following diagram shows this scenario. For information about other scenarios, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).



Your DB instance needs to be available only to your web server, and not to the public internet. Thus, you create a VPC with both public and private subnets. The web server is hosted in the public subnet, so that it can reach the public internet. The DB instance is hosted in a private subnet. The web server can connect to the DB instance because it is hosted within the same VPC. But the DB instance isn't available to the public internet, providing greater security.

This tutorial configures an additional public and private subnet in a separate Availability Zone. These subnets aren't used by the tutorial. An RDS DB subnet group requires a subnet in at least two Availability Zones. The additional subnet makes it easier to switch to a Multi-AZ DB instance deployment in the future.

This tutorial describes configuring a VPC for Amazon RDS DB instances. For a tutorial that shows you how to create a web server for this VPC scenario, see [Tutorial: Create a web server and an Amazon RDS DB instance \(p. 198\)](#). For more information about Amazon VPC, see [Amazon VPC Getting Started Guide](#) and [Amazon VPC User Guide](#).

Tip

You can set up network connectivity between an Amazon EC2 instance and a DB instance automatically when you create the DB instance. The network configuration is similar to the one described in this tutorial. For more information, see [Configure automatic network connectivity with an EC2 instance \(p. 230\)](#).

Create a VPC with private and public subnets

Use the following procedure to create a VPC with both public and private subnets.

To create a VPC and subnets

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the top-right corner of the AWS Management Console, choose the Region to create your VPC in. This example uses the US West (Oregon) Region.
3. In the upper-left corner, choose **VPC dashboard**. To begin creating a VPC, choose **Create VPC**.
4. For **Resources to create** under **VPC settings**, choose **VPC and more**.
5. For the **VPC settings**, set these values:
 - **Name tag auto-generation – tutorial**
 - **IPv4 CIDR block – 10.0.0.0/16**
 - **IPv6 CIDR block – No IPv6 CIDR block**
 - **Tenancy – Default**
 - **Number of Availability Zones (AZs) – 2**
 - **Customize AZs** – Keep the default values.
 - **Number of public subnet – 2**
 - **Number of private subnets – 2**
 - **Customize subnets CIDR blocks** – Keep the default values.
 - **NAT gateways (\$)** – **None**
 - **VPC endpoints** – **None**
 - **DNS options** – Keep the default values.

Note

Amazon RDS requires at least two subnets in two different Availability Zones to support Multi-AZ DB instance deployments. This tutorial creates a Single-AZ deployment, but the requirement makes it easier to convert to a Multi-AZ DB instance in the future.

6. Choose **Create VPC**.

Create a VPC security group for a public web server

Next, you create a security group for public access. To connect to public EC2 instances in your VPC, you add inbound rules to your VPC security group. These allow traffic to connect from the internet.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.
3. On the **Create security group** page, set these values:
 - **Security group name: tutorial-securitygroup**

- **Description: Tutorial Security Group**
 - **VPC:** Choose the VPC that you created earlier, for example: **vpc-*identifier* (tutorial-vpc)**
4. Add inbound rules to the security group.
 - a. Determine the IP address to use to connect to EC2 instances in your VPC using Secure Shell (SSH). To determine your public IP address, in a different browser window or tab, you can use the service at <https://checkip.amazonaws.com>. An example of an IP address is **203.0.113.25/32**.

In many cases, you might connect through an internet service provider (ISP) or from behind your firewall without a static IP address. If so, find the range of IP addresses used by client computers.

Warning
If you use **0.0.0.0/0** for SSH access, you make it possible for all IP addresses to access your public instances using SSH. This approach is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, authorize only a specific IP address or range of addresses to access your instances using SSH.

 - b. In the **Inbound rules** section, choose **Add rule**.
 - c. Set the following values for your new inbound rule to allow SSH access to your Amazon EC2 instance. If you do this, you can connect to your Amazon EC2 instance to install the web server and other utilities. You also connect to your EC2 instance to upload content for your web server.
 - **Type: SSH**
 - **Source:** The IP address or range from Step a, for example: **203.0.113.25/32**.
 - d. Choose **Add rule**.
 - e. Set the following values for your new inbound rule to allow HTTP access to your web server:
 - **Type: HTTP**
 - **Source: 0.0.0.0/0**
 5. Choose **Create security group** to create the security group.

Note the security group ID because you need it later in this tutorial.

Create a VPC security group for a private DB instance

To keep your DB instance private, create a second security group for private access. To connect to private DB instances in your VPC, you add inbound rules to your VPC security group that allow traffic from your web server only.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.
3. On the **Create security group** page, set these values:
 - **Security group name: tutorial-db-securitygroup**
 - **Description: Tutorial DB Instance Security Group**
 - **VPC:** Choose the VPC that you created earlier, for example: **vpc-*identifier* (tutorial-vpc)**
4. Add inbound rules to the security group.
 - a. In the **Inbound rules** section, choose **Add rule**.
 - b. Set the following values for your new inbound rule to allow MySQL traffic on port 3306 from your Amazon EC2 instance. If you do this, you can connect from your web server to your DB

instance. By doing so, you can store and retrieve data from your web application to your database.

- **Type:** MySQL/Aurora
 - **Source:** The identifier of the **tutorial-securitygroup** security group that you created previously in this tutorial, for example: **sg-9edd5cfb**.
5. Choose **Create security group** to create the security group.

Create a DB subnet group

A *DB subnet group* is a collection of subnets that you create in a VPC and that you then designate for your DB instances. A DB subnet group makes it possible for you to specify a particular VPC when creating DB instances.

To create a DB subnet group

1. Identify the private subnets for your database in the VPC.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **Subnets**.
 - c. Note the subnet IDs of the subnets named **tutorial-subnet-private1-us-west-2a** and **tutorial-subnet-private2-us-west-2b**.

You need the subnet IDs when you create your DB subnet group.

2. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

Make sure that you connect to the Amazon RDS console, not to the Amazon VPC console.

3. In the navigation pane, choose **Subnet groups**.
4. Choose **Create DB subnet group**.
5. On the **Create DB subnet group** page, set these values in **Subnet group details**:

- **Name:** **tutorial-db-subnet-group**
- **Description:** **Tutorial DB Subnet Group**
- **VPC:** **tutorial-vpc (vpc-*identifier*)**

6. In the **Add subnets** section, choose the **Availability Zones** and **Subnets**.

For this tutorial, choose **us-west-2a** and **us-west-2b** for the **Availability Zones**. For **Subnets**, choose the private subnets you identified in the previous step.

7. Choose **Create**.

Your new DB subnet group appears in the DB subnet groups list on the RDS console. You can choose the DB subnet group to see details in the details pane at the bottom of the window. These details include all of the subnets associated with the group.

Note

If you created this VPC to complete [Tutorial: Create a web server and an Amazon RDS DB instance \(p. 198\)](#), create the DB instance by following the instructions in [Create a DB instance \(p. 203\)](#).

Deleting the VPC

After you create the VPC and other resources for this tutorial, you can delete them if they are no longer needed.

Note

If you added resources in the VPC that you created for this tutorial, you might need to delete these before you can delete the VPC. For example, these resources might include Amazon EC2 instances or Amazon RDS DB instances. For more information, see [Delete your VPC](#) in the *Amazon VPC User Guide*.

To delete a VPC and related resources

1. Delete the DB subnet group.
 - a. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
 - b. In the navigation pane, choose **Subnet groups**.
 - c. Select the DB subnet group you want to delete, such as **tutorial-db-subnet-group**.
 - d. Choose **Delete**, and then choose **Delete** in the confirmation window.
2. Note the VPC ID.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **VPCs**.
 - c. In the list, identify the VPC that you created, such as **tutorial-vpc**.
 - d. Note the **VPC ID** of the VPC that you created. You need the VPC ID in later steps.
3. Delete the security groups.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **Security Groups**.
 - c. Select the security group for the Amazon RDS DB instance, such as **tutorial-db-securitygroup**.
 - d. For **Actions**, choose **Delete security groups**, and then choose **Delete** on the confirmation page.
 - e. On the **Security Groups** page, select the security group for the Amazon EC2 instance, such as **tutorial-securitygroup**.
 - f. For **Actions**, choose **Delete security groups**, and then choose **Delete** on the confirmation page.
4. Delete the NAT gateway.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **NAT Gateways**.
 - c. Select the NAT gateway of the VPC that you created. Use the VPC ID to identify the correct NAT gateway.
 - d. For **Actions**, choose **Delete NAT gateway**.
 - e. On the confirmation page, enter **delete**, and then choose **Delete**.
5. Delete the VPC.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **VPCs**.
 - c. Select the VPC you want to delete, such as **tutorial-vpc**.
 - d. For **Actions**, choose **Delete VPC**.

The confirmation page shows other resources that are associated with the VPC that will also be deleted, including the subnets associated with it.

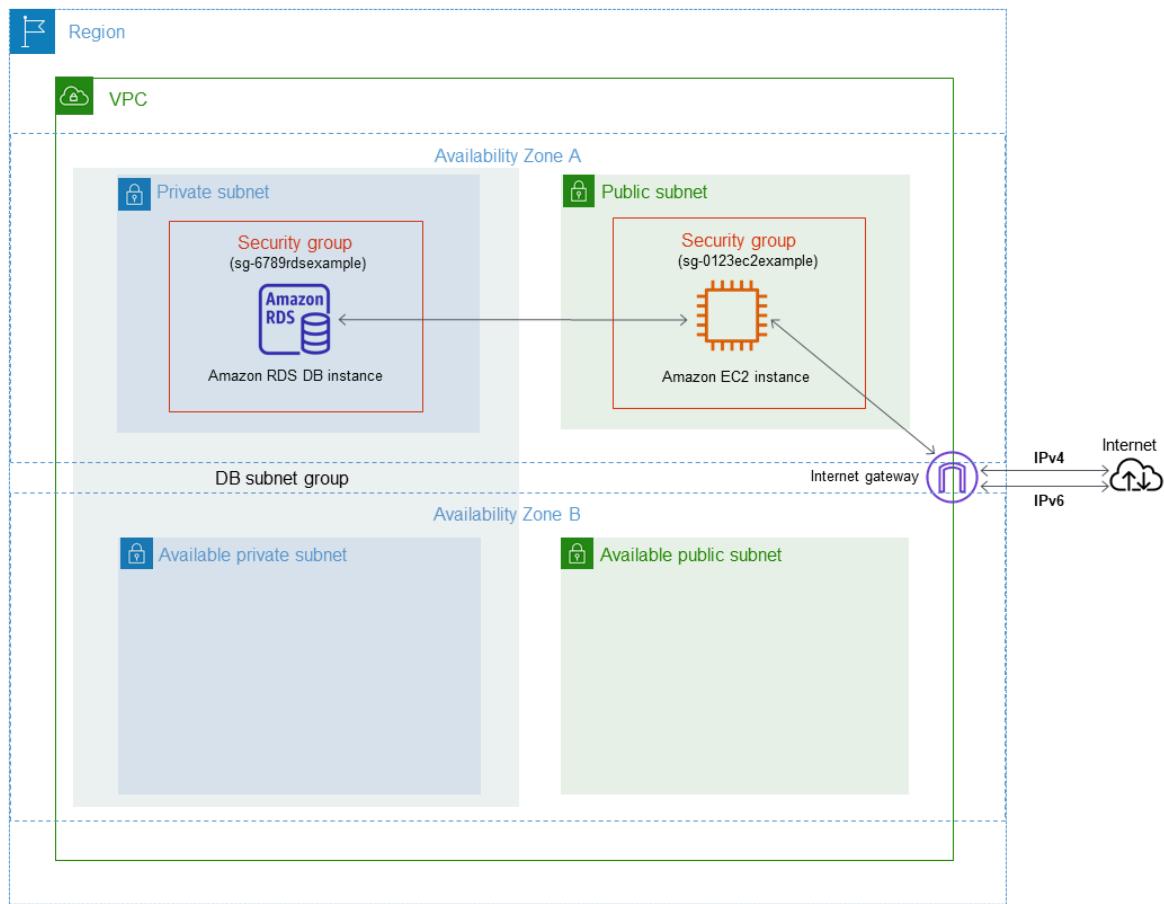
 - e. On the confirmation page, enter **delete**, and then choose **Delete**.
6. Release the Elastic IP addresses:
 - a. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
 - b. Choose **Amazon EC2 Dashboard**, and then choose **Elastic IPs**.
 - c. Select the Elastic IP address you want to release.

- d. For **Actions**, choose **Release Elastic IP addresses**.
- e. On the confirmation page, choose **Release**.

Tutorial: Create a VPC for use with a DB instance (dual-stack mode)

A common scenario includes a DB instance in a virtual private cloud (VPC) based on the Amazon VPC service. This VPC shares data with a public Amazon EC2 instance that is running in the same VPC. In this tutorial, you create the VPC for this scenario that works with a database running in dual-stack mode.

The following diagram shows this scenario.



For information about other scenarios, see [Scenarios for accessing a DB instance in a VPC \(p. 2115\)](#).

Your DB instance needs to be available only to your Amazon EC2 instance, and not to the public internet. Thus, you create a VPC with both public and private subnets. The Amazon EC2 instance is hosted in the public subnet, so that it can reach the public internet. The DB instance is hosted in a private subnet. The Amazon EC2 instance can connect to the DB instance because it's hosted within the same VPC. However, the DB instance is not available to the public internet, providing greater security.

This tutorial configures an additional public and private subnet in a separate Availability Zone. These subnets aren't used by the tutorial. An RDS subnet group requires a subnet in at least two Availability Zones. The additional subnet makes it easy to switch to a Multi-AZ DB instance deployment in the future.

To create a DB instance that uses dual-stack mode, specify **Dual-stack mode** for the **Network type** setting. You can also modify a DB instance with the same setting. For more information, see [Creating an Amazon RDS DB instance \(p. 230\)](#) and [Modifying an Amazon RDS DB instance \(p. 327\)](#).

This tutorial describes configuring a VPC for Amazon RDS DB instances. For more information about Amazon VPC, see [Amazon VPC Getting Started Guide](#) and [Amazon VPC User Guide](#).

Create a VPC with private and public subnets

Use the following procedure to create a VPC with both public and private subnets.

To create a VPC and subnets

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. In the upper-right corner of the AWS Management Console, choose the Region to create your VPC in. This example uses the US East (Ohio) Region.
3. In the upper-left corner, choose **VPC dashboard**. To begin creating a VPC, choose **Create VPC**.
4. For **Resources to create** under **VPC settings**, choose **VPC and more**.
5. For the remaining **VPC settings**, set these values:
 - **Name tag auto-generation – tutorial-dual-stack**
 - **IPv4 CIDR block – 10.0.0.0/16**
 - **IPv6 CIDR block – Amazon-provided IPv6 CIDR block**
 - **Tenancy – Default**
 - **Number of Availability Zones (AZs) – 2**
 - **Customize AZs** – Keep the default values.
 - **Number of public subnet – 2**
 - **Number of private subnets – 2**
 - **Customize subnets CIDR blocks** – Keep the default values.
 - **NAT gateways (\$)** – None
 - **Egress only internet gateway – No**
 - **VPC endpoints – None**
 - **DNS options** – Keep the default values.

Note

Amazon RDS requires at least two subnets in two different Availability Zones to support Multi-AZ DB instance deployments. This tutorial creates a Single-AZ deployment, but the requirement makes it easy to convert to a Multi-AZ DB instance deployment in the future.

6. Choose **Create VPC**.

Create a VPC security group for a public Amazon EC2 instance

Next, you create a security group for public access. To connect to public EC2 instances in your VPC, add inbound rules to your VPC security group that allow traffic to connect from the internet.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.
3. On the **Create security group** page, set these values:
 - **Security group name: tutorial-dual-stack-securitygroup**
 - **Description: Tutorial Dual-Stack Security Group**

- **VPC:** Choose the VPC that you created earlier, for example: `vpc-identifier (tutorial-dual-stack-vpc)`
- 4. Add inbound rules to the security group.

- a. Determine the IP address to use to connect to EC2 instances in your VPC using Secure Shell (SSH).

To determine your public IP address, in a different browser window or tab use the service at <https://checkip.amazonaws.com>. An example of an Internet Protocol version 4 (IPv4) address is `203.0.113.25/32`. An example of an Internet Protocol version 6 (IPv6) address is `2001:DB8::/32`.

In many cases, you might connect through an internet service provider (ISP) or from behind your firewall without a static IP address. If so, find the range of IP addresses used by client computers.

Warning

If you use `0.0.0.0/0` for IPv4 or `::0` for IPv6, you make it possible for all IP addresses to access your public instances using SSH. This approach is acceptable for a short time in a test environment, but it's unsafe for production environments. In production, authorize only a specific IP address or range of addresses to access your instances.

- b. In the **Inbound rules** section, choose **Add rule**.
- c. Set the following values for your new inbound rule to allow Secure Shell (SSH) access to your Amazon EC2 instance. If you do this, you can connect to your EC2 instance to install SQL clients and other applications. Specify an IP address so you can access your EC2 instance:
 - **Type:** SSH
 - **Source:** The IP address or range from step a. An example of an IPv4 IP address is `203.0.113.25/32`. An example of an IPv6 IP address is `2001:DB8::/32`.

5. Choose **Create security group** to create the security group.

Note the security group ID because you need it later in this tutorial.

Create a VPC security group for a private DB instance

To keep your DB instance private, create a second security group for private access. To connect to private DB instances in your VPC, add inbound rules to your VPC security group. These allow traffic from your Amazon EC2 instance only.

To create a VPC security group

1. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
2. Choose **VPC Dashboard**, choose **Security Groups**, and then choose **Create security group**.
3. On the **Create security group** page, set these values:
 - **Security group name:** `tutorial-dual-stack-db-securitygroup`
 - **Description:** Tutorial Dual-Stack DB Instance Security Group
 - **VPC:** Choose the VPC that you created earlier, for example: `vpc-identifier (tutorial-dual-stack-vpc)`
4. Add inbound rules to the security group:
 - a. In the **Inbound rules** section, choose **Add rule**.
 - b. Set the following values for your new inbound rule to allow MySQL traffic on port 3306 from your Amazon EC2 instance. If you do, you can connect from your EC2 instance to your DB

instance. Doing this means that you can store and retrieve data from your EC2 instance to your database.

- **Type:** MySQL/Aurora
 - **Source:** The identifier of the **tutorial-dual-stack-securitygroup** security group that you created previously in this tutorial, for example **sg-9edd5cfb**.
5. To create the security group, choose **Create security group**.

Create a DB subnet group

A *DB subnet group* is a collection of subnets that you create in a VPC and that you then designate for your DB instances. By using a DB subnet group, you can specify a particular VPC when creating DB instances. To create a DB subnet group that is DUAL compatible, all subnets must be DUAL compatible. To be DUAL compatible, a subnet must have an IPv6 CIDR associated with it.

To create a DB subnet group

1. Identify the private subnets for your database in the VPC.
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **Subnets**.
 - c. Note the subnet IDs of the subnets named **tutorial-dual-stack-subnet-private1-us-west-2a** and **tutorial-dual-stack-subnet-private2-us-west-2b**.

You will need the subnet IDs when you create your DB subnet group.

2. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.

Make sure that you connect to the Amazon RDS console, not to the Amazon VPC console.

3. In the navigation pane, choose **Subnet groups**.
4. Choose **Create DB subnet group**.
5. On the **Create DB subnet group** page, set these values in **Subnet group details**:
 - **Name:** **tutorial-dual-stack-db-subnet-group**
 - **Description:** **Tutorial Dual-Stack DB Subnet Group**
 - **VPC:** **tutorial-dual-stack-vpc (vpc-*identifier*)**
6. In the **Add subnets** section, choose values for the **Availability Zones** and **Subnets** options.

For this tutorial, choose **us-east-2a** and **us-east-2b** for the **Availability Zones**. For **Subnets**, choose the private subnets you identified in the previous step.

7. Choose **Create**.

Your new DB subnet group appears in the DB subnet groups list on the RDS console. You can choose the DB subnet group to see its details. These include the supported addressing protocols and all of the subnets associated with the group and the network type supported by the DB subnet group.

Create an Amazon EC2 instance in dual-stack mode

To create an Amazon EC2 instance, follow the instructions in [Launch an instance using the new launch instance wizard](#) in the *Amazon EC2 User Guide for Linux Instances*.

On the **Configure Instance Details** page, set these values and keep the other values as their defaults:

- **Network** – Choose the VPC with both public and private subnets that you chose for the DB instance, such as `vpc-identifier` | `tutorial-dual-stack-vpc` created in [Create a VPC with private and public subnets \(p. 2127\)](#).
- **Subnet** – Choose an existing public subnet, such as `subnet-identifier` | `tutorial-dual-stack-subnet-public1-us-east-2a` | `us-east-2a` created in [Create a VPC security group for a public Amazon EC2 instance \(p. 2127\)](#).
- **Auto-assign Public IP** – Choose **Enable**.
- **Auto-assign IPv6 IP** – Choose **Enable**.
- **Firewall (security groups)** – Choose **Select an existing security group**.
- **Common security groups** – Choose an existing security group, such as the `tutorial-securitygroup` created in [Create a VPC security group for a public Amazon EC2 instance \(p. 2127\)](#). Make sure that the security group that you choose includes inbound rules for Secure Shell (SSH) and HTTP access.

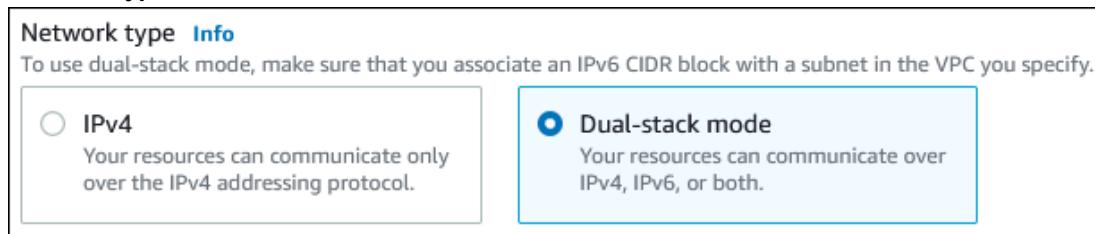
Create a DB instance in dual-stack mode

In this step, you create a DB instance that runs in dual-stack mode.

To create a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the console, choose the AWS Region where you want to create the DB instance. This example uses the US East (Ohio) Region.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.
5. On the **Create database** page, make sure that the **Standard create** option is chosen, and then choose the MySQL DB engine type.
6. In the **Connectivity** section, set these values:

- **Network type** – Choose **Dual-stack mode**.



- **Virtual private cloud (VPC)** – Choose an existing VPC with both public and private subnets, such as `tutorial-dual-stack-vpc` (`vpc-identifier`) created in [Create a VPC with private and public subnets \(p. 2127\)](#).

The VPC must have subnets in different Availability Zones.

- **DB subnet group** – Choose a DB subnet group for the VPC, such as `tutorial-dual-stack-db-subnet-group` created in [Create a DB subnet group \(p. 2129\)](#).
- **Public access** – Choose **No**.
- **VPC security group (firewall)** – Select **Choose existing**.
- **Existing VPC security groups** – Choose an existing VPC security group that is configured for private access, such as `tutorial-dual-stack-db-securitygroup` created in [Create a VPC security group for a private DB instance \(p. 2128\)](#).

Remove other security groups, such as the default security group, by choosing the **X** associated with each.

- **Availability Zone** – Choose **us-west-2a**.

To avoid cross-AZ traffic, make sure the DB instance and the EC2 instance are in the same Availability Zone.

7. For the remaining sections, specify your DB instance settings. For information about each setting, see [Settings for DB instances \(p. 237\)](#).

Connect to your Amazon EC2 instance and DB instance

After you create your Amazon EC2 instance and DB instance in dual-stack mode, you can connect to each one using the IPv6 protocol. To connect to an Amazon EC2 instance using the IPv6 protocol, follow the instructions in [Connect to your Linux instance](#) in the *Amazon EC2 User Guide for Linux Instances*.

To connect to your DB instance, follow the instructions in [Connecting to an Amazon RDS DB instance \(p. 267\)](#).

Deleting the VPC

After you create the VPC and other resources for this tutorial, you can delete them if they are no longer needed.

If you added resources in the VPC that you created for this tutorial, you might need to delete these before you can delete the VPC. Examples of resources are Amazon EC2 instances or DB instances. For more information, see [Delete your VPC](#) in the *Amazon VPC User Guide*.

To delete a VPC and related resources

1. Delete the DB subnet group:
 - a. Open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
 - b. In the navigation pane, choose **Subnet groups**.
 - c. Select the DB subnet group to delete, such as **tutorial-db-subnet-group**.
 - d. Choose **Delete**, and then choose **Delete** in the confirmation window.
2. Note the VPC ID:
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **VPCs**.
 - c. In the list, identify the VPC you created, such as **tutorial-dual-stack-vpc**.
 - d. Note the **VPC ID** value of the VPC that you created. You need this VPC ID in subsequent steps.
3. Delete the security groups:
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **Security Groups**.
 - c. Select the security group for the Amazon RDS DB instance, such as **tutorial-dual-stack-db-securitygroup**.
 - d. For **Actions**, choose **Delete security groups**, and then choose **Delete** on the confirmation page.
 - e. On the **Security Groups** page, select the security group for the Amazon EC2 instance, such as **tutorial-dual-stack-securitygroup**.
 - f. For **Actions**, choose **Delete security groups**, and then choose **Delete** on the confirmation page.
4. Delete the NAT gateway:

-
- a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **NAT Gateways**.
 - c. Select the NAT gateway of the VPC that you created. Use the VPC ID to identify the correct NAT gateway.
 - d. For **Actions**, choose **Delete NAT gateway**.
 - e. On the confirmation page, enter **delete**, and then choose **Delete**.
5. Delete the VPC:
 - a. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
 - b. Choose **VPC Dashboard**, and then choose **VPCs**.
 - c. Select the VPC that you want to delete, such as **tutorial-dual-stack-vpc**.
 - d. For **Actions**, choose **Delete VPC**.
 - The confirmation page shows other resources that are associated with the VPC that will also be deleted, including the subnets associated with it.
 - e. On the confirmation page, enter **delete**, and then choose **Delete**.
6. Release the Elastic IP addresses:
 - a. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
 - b. Choose **EC2 Dashboard**, and then choose **Elastic IPs**.
 - c. Select the Elastic IP address that you want to release.
 - d. For **Actions**, choose **Release Elastic IP addresses**.
 - e. On the confirmation page, choose **Release**.

Moving a DB instance not in a VPC into a VPC

Some legacy DB instances on the EC2-Classic platform are not in a VPC. If your DB instance is not in a VPC, you can use the AWS Management Console to easily move your DB instance into a VPC. Before you can move a DB instance not in a VPC, into a VPC, you must create the VPC.

EC2-Classic was retired on August 15, 2022. If you haven't migrated from EC2-Classic to a VPC, we recommend that you migrate as soon as possible. For more information, see [Migrate from EC2-Classic to a VPC](#) in the *Amazon EC2 User Guide* and the blog [EC2-Classic Networking is Retiring – Here's How to Prepare](#).

Important

If you are a new Amazon RDS customer, if you have never created a DB instance before, or if you are creating a DB instance in an AWS Region you have not used before, in almost all cases you are on the EC2-VPC platform and have a default VPC. For information about working with DB instances in a VPC, see [Working with a DB instance in a VPC \(p. 2103\)](#).

Follow these steps to create a VPC for your DB instance.

- [Step 1: Create a VPC \(p. 2111\)](#)
- [Step 2: Create a DB subnet group \(p. 2111\)](#)
- [Step 3: Create a VPC security group \(p. 2114\)](#)

After you create the VPC, follow these steps to move your DB instance into the VPC.

- [Updating the VPC for a DB instance \(p. 2114\)](#)

We highly recommend that you create a backup of your DB instance immediately before the migration. Doing so ensures that you can restore the data if the migration fails. For more information, see [Backing up and restoring an Amazon RDS DB instance \(p. 426\)](#).

The following are some limitations to moving your DB instance into the VPC.

- **Previous generation DB instance classes** – Previous generation DB instance classes might not be supported on the VPC platform. When moving a DB instance to a VPC, choose a db.m3 or db.r3 DB instance class. After you move the DB instance to a VPC, you can scale the DB instance to use a later DB instance class. For a full list of VPC supported instance classes, see [Amazon RDS instance types](#).
- **Multi-AZ** – Moving a Multi-AZ DB instance not in a VPC into a VPC is not currently supported. To move your DB instance to a VPC, first modify the DB instance so that it is a single-AZ deployment. Change the **Multi-AZ deployment** setting to **No**. After you move the DB instance to a VPC, modify it again to make it a Multi-AZ deployment. For more information, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).
- **Read replicas** – Moving a DB instance with read replicas not in a VPC into a VPC is not currently supported. To move your DB instance to a VPC, first delete all of its read replicas. After you move the DB instance to a VPC, recreate the read replicas. For more information, see [Working with read replicas \(p. 370\)](#).
- **Option groups** – If you move your DB instance to a VPC, and the DB instance is using a custom option group, change the option group that is associated with your DB instance. Option groups are platform-specific, and moving to a VPC is a change in platform. To use a custom option group in this case, assign the default VPC option group to the DB instance, assign an option group that is used by other DB instances in the VPC you are moving to, or create a new option group and assign it to the DB instance. For more information, see [Working with option groups \(p. 273\)](#).

Alternatives for moving a DB instance not in a VPC into a VPC with minimal downtime

Using the following alternatives, you can move a DB instance not in a VPC into a VPC with minimal downtime. These alternatives cause minimum disruption to the source DB instance and allow it to serve user traffic during the migration. However, the time required to migrate to a VPC will vary based on the database size and the live workload characteristics.

- **AWS Database Migration Service (AWS DMS)** – AWS DMS enables the live migration of data while keeping the source DB instance fully operational, but it replicates only a limited set of DDL statements. AWS DMS doesn't propagate items such as indexes, users, privileges, stored procedures, and other database changes not directly related to table data. In addition, AWS DMS doesn't automatically use RDS snapshots for the initial DB instance creation, which can increase migration time. For more information, see [AWS Database Migration Service](#).
- **DB snapshot restore or point-in-time recovery** – You can move a DB instance to a VPC by restoring a snapshot of the DB instance or by restoring a DB instance to a point in time. For more information, see [Restoring from a DB snapshot \(p. 452\)](#) and [Restoring a DB instance to a specified time \(p. 499\)](#).

Quotas and constraints for Amazon RDS

Following, you can find a description of the resource quotas and naming constraints for Amazon RDS.

Topics

- [Quotas in Amazon RDS \(p. 2135\)](#)
- [Naming constraints in Amazon RDS \(p. 2138\)](#)
- [Maximum number of database connections \(p. 2139\)](#)
- [File size limits in Amazon RDS \(p. 2140\)](#)

Quotas in Amazon RDS

Each AWS account has quotas, for each AWS Region, on the number of Amazon RDS resources that can be created. After a quota for a resource has been reached, additional calls to create that resource fail with an exception.

The following table lists the resources and their quotas per AWS Region.

Name	Default	Adjust	Description
Authorizations per DB security group	Each supported Region: 20	No	Number of security group authorizations per DB security group
Custom engine versions	Each supported Region: 40	Yes	The maximum number of custom engine versions allowed in this account in the current Region
DB cluster parameter groups	Each supported Region: 50	No	The maximum number of DB cluster parameter groups
DB clusters	Each supported Region: 40	Yes	The maximum number of Aurora clusters allowed in this account in the current Region
DB instances	Each supported Region: 40	Yes	The maximum number of DB instances allowed in this account in the current Region
DB subnet groups	Each supported Region: 50	Yes	The maximum number of DB subnet groups
Data API HTTP request body size	Each supported Region: 4 Megabytes	No	The maximum size allowed for the HTTP request body.

Name	Default	Adjust	Description
Data API maximum concurrent cluster-secret pairs	Each supported Region: 30	No	The maximum number of unique pairs of Aurora Serverless DB clusters and secrets in concurrent Data API requests for the current account and AWS Region.
Data API maximum concurrent requests	Each supported Region: 500	No	The maximum number of Data API requests to an Aurora Serverless DB cluster that use the same secret and can be processed at the same time. Additional requests are queued and processed as in-process requests complete.
Data API maximum result set size	Each supported Region: 1 Megabytes	No	The maximum size of the database result set that can be returned by the Data API.
Data API maximum size of JSON response string	Each supported Region: 10 Megabytes	No	The maximum size of the simplified JSON response string returned by the RDS Data API.
Data API requests per second	Each supported Region: 1,000 per second	No	The maximum number of requests to the Data API per second allowed in this account in the current AWS Region.
Event subscriptions	Each supported Region: 20	Yes	The maximum number of event subscriptions
IAM roles per DB cluster	Each supported Region: 5	Yes	The maximum number of IAM roles associated with a DB cluster
IAM roles per DB instance	Each supported Region: 5	Yes	The maximum number of IAM roles associated with a DB instance
Manual DB cluster snapshots	Each supported Region: 100	Yes	The maximum number of manual DB cluster snapshots
Manual DB instance snapshots	Each supported Region: 100	Yes	The maximum number of manual DB instance snapshots
Option groups	Each supported Region: 20	Yes	The maximum number of option groups

Name	Default	Adjust	Description
Parameter groups	Each supported Region: 50	Yes	The maximum number of parameter groups
Proxies	Each supported Region: 20	Yes	The maximum number of proxies allowed in this account in the current AWS Region
Read replicas per master	Each supported Region: 15	Yes	The maximum number of read replicas per master
Reserved DB instances	Each supported Region: 40	Yes	The maximum number of reserved DB instances allowed in this account in the current AWS Region
Rules per security group	Each supported Region: 20	No	The maximum number of rules per DB security group
Security groups	Each supported Region: 25	Yes	The maximum number of DB security groups
Security groups (VPC)	Each supported Region: 5	No	The maximum number of DB security groups per Amazon VPC
Subnets per DB subnet group	Each supported Region: 20	No	The maximum number of subnets per DB subnet group
Tags per resource	Each supported Region: 50	No	The maximum number of tags per Amazon RDS resource
Total storage for all DB instances	Each supported Region: 100,000 Gigabytes	Yes	The maximum total storage (in GB) for all DB instances added together

Note

By default, you can have up to a total of 40 DB instances. RDS DB instances, Aurora DB instances, Amazon Neptune instances, and Amazon DocumentDB instances apply to this quota. The following limitations apply to the Amazon RDS DB instances:

- 10 for each SQL Server edition (Enterprise, Standard, Web, and Express) under the "license-included" model
- 10 for Oracle under the "license-included" model
- 40 for MySQL, MariaDB, or PostgreSQL
- 40 for Oracle under the "bring-your-own-license" (BYOL) licensing model

If your application requires more DB instances, you can request additional DB instances by opening the [Service Quotas console](#). In the navigation pane, choose **AWS services**. Choose **Amazon Relational Database Service (Amazon RDS)**, choose a quota, and follow the directions to request a quota increase. For more information, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

For RDS for Oracle and RDS for SQL Server, the read replica limit is 5 per source database for each Region.

Backups managed by AWS Backup are considered manual DB snapshots, but don't count toward the manual snapshot quota. For information about AWS Backup, see the [AWS Backup Developer Guide](#).

If you use any RDS API operations and exceed the default quota for the number of calls per second, the Amazon RDS API issues an error like the following one.

ClientError: An error occurred (ThrottlingException) when calling the *API_name* operation: Rate exceeded.

Here, reduce the number of calls per second. The quota is meant to cover most use cases. If higher limits are needed, request a quota increase by contacting AWS Support. Open the [AWS Support Center](#) page, sign in if necessary, and choose **Create case**. Choose **Service limit increase**. Complete and submit the form.

Note

This quota can't be changed in the Amazon RDS Service Quotas console.

Naming constraints in Amazon RDS

The following table describes naming constraints in Amazon RDS.

Resource or item	Constraints
DB instance identifier	Identifiers have these naming constraints: <ul style="list-style-type: none">Must contain 1–63 alphanumeric characters or hyphens.First character must be a letter.Can't end with a hyphen or contain two consecutive hyphens.Must be unique for all DB instances per AWS account, per AWS Region.
Database name	Database name constraints differ for each database engine . For more information, see the available settings when creating each DB instance. <p>Note This approach doesn't apply to SQL Server. For SQL Server, you create your databases after you create your DB instance.</p>
Master user name	Master user name constraints differ for each database engine. For more information, see the available settings when creating each DB instance.
Master password	The password for the database master user can include any printable ASCII character except /, ', ", @, or a space. The password has the following number of printable ASCII characters depending on the DB engine: <ul style="list-style-type: none">MariaDB and MySQL: 8–41Oracle: 8–30SQL Server and PostgreSQL: 8–128

Resource or item	Constraints
DB parameter group name	<p>These names have these constraints:</p> <ul style="list-style-type: none"> • Must contain 1–255 alphanumeric characters. • First character must be a letter. • Hyphens are allowed, but the name cannot end with a hyphen or contain two consecutive hyphens.
DB subnet group name	<p>These names have these constraints:</p> <ul style="list-style-type: none"> • Must contain 1–255 characters. • Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

Maximum number of database connections

The maximum number of simultaneous database connections varies by the DB engine type and the memory allocation for the DB instance class. The maximum number of connections is generally set in the parameter group associated with the DB instance. The exception is Microsoft SQL Server, where it is set in the server properties for the DB instance in SQL Server Management Studio (SSMS).

`DBInstanceClassMemory` is in bytes. For details about how this value is calculated, see [Specifying DB parameters \(p. 310\)](#). Because of memory reserved for the operating system and RDS management processes, this memory size is smaller than the value in gibibytes (GiB) shown in [Hardware specifications for DB instance classes \(p. 55\)](#).

If your applications frequently open and close connections, or keep a large number of long-lived connections open, we recommend that you use Amazon RDS Proxy. RDS Proxy is a fully managed, highly available database proxy that uses connection pooling to share database connections securely and efficiently. To learn more about RDS Proxy, see [Using Amazon RDS Proxy \(p. 921\)](#).

Note

For Oracle, you set the maximum number of user processes and user and system sessions.

Maximum database connections

DB engine	Parameter	Allowed values	Default value	Description
MariaDB and MySQL	<code>max_connections</code>	1–100000	<p>Default for all MariaDB and MySQL versions except MariaDB version 10.6: $\{DBInstanceClassMemory/12582880\}$</p> <p>Default for MariaDB version 10.6: $\text{LEAST}\{\{DBInstanceClassMemory/25165760\}, 12000\}$</p> <p>Note If the default value calculation results in a value greater than 16,000, Amazon RDS sets</p>	Number of simultaneous client connections allowed

DB engine	Parameter	Allowed values	Default value	Description
			the limit to 16,000 for MariaDB and MySQL DB instances.	
Oracle	processes	80–20000	LEAST(DBInstanceClassMemory/12,582,880, 20000)	DB processes
	sessions	100–65535	–	User and system sessions
PostgreSQL	max_connections	6–8388607	LEAST(DBInstanceClassMemory/12,582,880, 5000)	Max concurrent connections
SQL Server	Maximum number of concurrent connections	0–32767	0 (unlimited)	Maximum number of concurrent connections

In some instances, the total RAM is 16 GiB, or 17,179,869,184 bytes. In these instances, the variable DBInstanceClassMemory automatically subtracts the amounts reserved to the operating system and the RDS processes that manage the instance. The remainder of the subtraction is then divided by 12,582,880. This results in the maximum connections number being around 1,300, depending on instance type, instance size, and DB engine.

Database connections consume memory. Setting one of these parameters too high can cause a low memory condition that might cause a DB instance to be placed in the **incompatible-parameters** status. For more information, see [Diagnosing and resolving incompatible parameters status for a memory limit \(p. 2148\)](#).

Note

You might see fewer than the maximum number of DB connections. This is to avoid potential out-of-memory issues.

File size limits in Amazon RDS

File size limits apply to certain Amazon RDS DB instances. For more information, see the following engine-specific limits:

- [MariaDB file size limits in Amazon RDS \(p. 1056\)](#)
- [MySQL file size limits in Amazon RDS \(p. 1437\)](#)
- [Oracle file size limits in Amazon RDS \(p. 1485\)](#)

Troubleshooting for Amazon RDS

Use the following sections to help troubleshoot problems you have with DB instances in Amazon RDS and Amazon Aurora.

Topics

- [Can't connect to Amazon RDS DB instance \(p. 2141\)](#)
- [Amazon RDS security issues \(p. 2143\)](#)
- [Resetting the DB instance owner password \(p. 2144\)](#)
- [Amazon RDS DB instance outage or reboot \(p. 2144\)](#)
- [Amazon RDS DB parameter changes not taking effect \(p. 2144\)](#)
- [Amazon RDS DB instance running out of storage \(p. 2145\)](#)
- [Amazon RDS insufficient DB instance capacity \(p. 2146\)](#)
- [Freeable memory issues in Amazon RDS \(p. 2146\)](#)
- [MySQL and MariaDB issues \(p. 2147\)](#)
- [Can't set backup retention period to 0 \(p. 2154\)](#)

For information about debugging problems using the Amazon RDS API, see [Troubleshooting applications on Amazon RDS \(p. 2155\)](#).

Can't connect to Amazon RDS DB instance

When you can't connect to a DB instance, the following are common causes:

- **Inbound rules** – The access rules enforced by your local firewall and the IP addresses authorized to access your DB instance might not match. The problem is most likely the inbound rules in your security group.

By default, DB instances don't allow access. Access is granted through a security group associated with the VPC that allows traffic into and out of the DB instance. If necessary, add inbound and outbound rules for your particular situation to the security group. You can specify an IP address, a range of IP addresses, or another VPC security group.

Note

When adding a new inbound rule, you can choose **My IP** for **Source** to allow access to the DB instance from the IP address detected in your browser.

For more information about setting up security groups, see [Provide access to your DB instance in your VPC by creating a security group \(p. 151\)](#).

Note

Client connections from IP addresses within the range 169.254.0.0/16 aren't permitted. This is the Automatic Private IP Addressing Range (APIPA), which is used for local-link addressing.

- **Public accessibility** – To connect to your DB instance from outside of the VPC, such as by using a client application, the instance must have a public IP address assigned to it.

To make the instance publicly accessible, modify it and choose **Yes** under **Public accessibility**. For more information, see [Hiding a DB instance in a VPC from the internet \(p. 2109\)](#).

- **Port** – The port that you specified when you created the DB instance can't be used to send or receive communications due to your local firewall restrictions. To determine if your network allows the specified port to be used for inbound and outbound communication, check with your network administrator.

- **Availability** – For a newly created DB instance, the DB instance has a status of *creating* until the DB instance is ready to use. When the state changes to *available*, you can connect to the DB instance. Depending on the size of your DB instance, it can take up to 20 minutes before an instance is available.
- **Internet gateway** – For a DB instance to be publicly accessible, the subnets in its DB subnet group must have an internet gateway.

To configure an internet gateway for a subnet

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**, and then choose the name of the DB instance.
3. In the **Connectivity & security** tab, write down the values of the VPC ID under **VPC** and the subnet ID under **Subnets**.
4. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/>.
5. In the navigation pane, choose **Internet Gateways**. Verify that there is an internet gateway attached to your VPC. Otherwise, choose **Create Internet Gateway** to create an internet gateway. Select the internet gateway, and then choose **Attach to VPC** and follow the directions to attach it to your VPC.
6. In the navigation pane, choose **Subnets**, and then select your subnet.
7. On the **Route Table** tab, verify that there is a route with **0.0.0.0/0** as the destination and the internet gateway for your VPC as the target.

If you're connecting to your instance using its IPv6 address, verify that there is a route for all IPv6 traffic (`::/0`) that points to the internet gateway. Otherwise, do the following:

- a. Choose the ID of the route table (rtb-xxxxxxx) to navigate to the route table.
- b. On the **Routes** tab, choose **Edit routes**. Choose **Add route**, use **0.0.0.0/0** as the destination and the internet gateway as the target.
For IPv6, choose **Add route**, use `::/0` as the destination and the internet gateway as the target.
- c. Choose **Save routes**.

Also, if you are trying to connect to IPv6 endpoint, make sure that client IPv6 address range is authorized to connect to the DB instance.

For more information, see [Working with a DB instance in a VPC \(p. 2103\)](#).

For engine-specific connection issues, see the following topics:

- [Troubleshooting connections to your SQL Server DB instance \(p. 1089\)](#)
- [Troubleshooting connections to your Oracle DB instance \(p. 1493\)](#)
- [Troubleshooting connections to your RDS for PostgreSQL instance \(p. 1814\)](#)
- [Maximum MySQL and MariaDB connections \(p. 2147\)](#)

Testing a connection to a DB instance

You can test your connection to a DB instance using common Linux or Microsoft Windows tools.

From a Linux or Unix terminal, you can test the connection by entering the following. Replace **DB-instance-endpoint** with the endpoint and **port** with the port of your DB instance.

```
nc -zv DB-instance-endpoint port
```

For example, the following shows a sample command and the return value.

```
nc -zv postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299
Connection to postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299 port [tcp/vvr-data] succeeded!
```

Windows users can use Telnet to test the connection to a DB instance. Telnet actions aren't supported other than for testing the connection. If a connection is successful, the action returns no message. If a connection isn't successful, you receive an error message such as the following.

```
C:\>telnet sg-postgresql1.c6c8mtnfake0.us-west-2.rds.amazonaws.com 819
Connecting To sg-postgresql1.c6c8mtnfake0.us-west-2.rds.amazonaws.com...Could not open
connection to the host, on port 819: Connect failed
```

If Telnet actions return success, your security group is properly configured.

Note

Amazon RDS doesn't accept internet control message protocol (ICMP) traffic, including ping.

Troubleshooting connection authentication

In some cases, you can connect to your DB instance but you get authentication errors. In these cases, you might want to reset the master user password for the DB instance. You can do this by modifying the RDS instance.

For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Amazon RDS security issues

To avoid security issues, never use your master AWS user name and password for a user account. Best practice is to use your master AWS account to create users and assign those to DB user accounts. You can also use your master account to create other user accounts, if necessary.

For information about creating IAM users, see [Creating an IAM user in your AWS account](#). For information about creating users in AWS IAM Identity Center (successor to AWS Single Sign-On), see [Manage identities in IAM Identity Center](#).

Error message "failed to retrieve account attributes, certain console functions may be impaired."

You can get this error for several reasons. It might be because your account is missing permissions, or your account hasn't been properly set up. If your account is new, you might not have waited for the account to be ready. If this is an existing account, you might lack permissions in your access policies to perform certain actions such as creating a DB instance. To fix the issue, your administrator needs to provide the necessary roles to your account. For more information, see [the IAM documentation](#).

Resetting the DB instance owner password

If you get locked out of your DB instance, you can log in as the master user. Then you can reset the credentials for other administrative users or roles. If you can't log in as the master user, the AWS account owner can reset the master user password. For details of which administrative accounts or roles you might need to reset, see [Master user account privileges \(p. 2087\)](#).

You can change the DB instance password by using the Amazon RDS console, the AWS CLI command [modify-db-instance](#), or by using the [ModifyDBInstance](#) API operation. For more information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Amazon RDS DB instance outage or reboot

A DB instance outage can occur when a DB instance is rebooted. It can also occur when the DB instance is put into a state that prevents access to it, and when the database is restarted. A reboot can occur when you manually reboot your DB instance. A reboot can also occur when you change a DB instance setting that requires a reboot before it can take effect.

A DB instance reboot occurs when you change a setting that requires a reboot, or when you manually cause a reboot. A reboot can occur immediately if you change a setting and request that the change take effect immediately. Or it can occur during the DB instance's maintenance window.

A DB instance reboot occurs immediately when one of the following occurs:

- You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0. You then set **Apply Immediately** to true.
- You change the DB instance class, and **Apply Immediately** is set to true.
- You change the storage type from **Magnetic (Standard)** to **General Purpose (SSD)** or **Provisioned IOPS (SSD)**, or from **Provisioned IOPS (SSD)** or **General Purpose (SSD)** to **Magnetic (Standard)**.

A DB instance reboot occurs during the maintenance window when one of the following occurs:

- You change the backup retention period for a DB instance from 0 to a nonzero value or from a nonzero value to 0, and **Apply Immediately** is set to false.
- You change the DB instance class, and **Apply Immediately** is set to false.

When you change a static parameter in a DB parameter group, the change doesn't take effect until the DB instance associated with the parameter group is rebooted. The change requires a manual reboot. The DB instance isn't automatically rebooted during the maintenance window.

To see a table that shows DB instance actions and the effect that setting the **Apply Immediately** value has, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Amazon RDS DB parameter changes not taking effect

In some cases, you might change a parameter in a DB parameter group but don't see the changes take effect. If so, you likely need to reboot the DB instance associated with the DB parameter group.

When you change a dynamic parameter, the change takes effect immediately. When you change a static parameter, the change doesn't take effect until you reboot the DB instance associated with the parameter group.

You can reboot a DB instance using the RDS console. Or you can explicitly call the [RebootDBInstance](#) API operation. You can reboot without failover if the DB instance is in a Multi-AZ deployment. The requirement to reboot the associated DB instance after a static parameter change helps mitigate the risk of a parameter misconfiguration affecting an API call. An example of this is calling [ModifyDBInstance](#) to change the DB instance class. For more information, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

Amazon RDS DB instance running out of storage

If your DB instance runs out of storage space, it might no longer be available. We highly recommend that you constantly monitor the `FreeStorageSpace` metric published in CloudWatch to make sure that your DB instance has enough free storage space.

If your database instance runs out of storage, its status changes to `storage-full`. For example, a call to the `DescribeDBInstances` API operation for a DB instance that has used up its storage outputs the following.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance

DBINSTANCE mydbinstance 2009-12-22T23:06:11.915Z db.m5.large mysql8.0 50 sa
storage-full mydbinstance.clla4j4jgyp.us-east-1.rds.amazonaws.com 3306
us-east-1b 3
SECGROUP default active
PARAMGRP default.mysql8.0 in-sync
```

To recover from this scenario, add more storage space to your instance using the `ModifyDBInstance` API operation or the following AWS CLI command.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--allocated-storage 60 \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--allocated-storage 60 ^
--apply-immediately
```

```
DBINSTANCE mydbinstance 2009-12-22T23:06:11.915Z db.m5.large mysql8.0 50 sa
storage-full mydbinstance.clla4j4jgyp.us-east-1.rds.amazonaws.com 3306
us-east-1b 3 60
SECGROUP default active
PARAMGRP default.mysql8.0 in-sync
```

Now, when you describe your DB instance, you see that your DB instance has `modifying` status, which indicates the storage is being scaled.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

```
DBINSTANCE mydbinstance 2009-12-22T23:06:11.915Z db.m5.large mysql8.0 50 sa
modifying mydbinstance.clla4j4jgyp.us-east-1.rds.amazonaws.com
3306 us-east-1b 3 60
SECGROUP default active
PARAMGRP default.mysql8.0 in-sync
```

After storage scaling is complete, your DB instance status changes to available.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

```
DBINSTANCE mydbinstance 2009-12-22T23:06:11.915Z db.m5.large mysql8.0 60 sa
available mydbinstance.clla4j4jgyp.us-east-1.rds.amazonaws.com 3306
us-east-1b 3
SECGROUP default active
PARAMGRP default.mysql8.0 in-sync
```

You can receive notifications when your storage space is exhausted using the `DescribeEvents` operation. For example, in this scenario, if you make a `DescribeEvents` call after these operations you see the following output.

```
aws rds describe-events --source-type db-instance --source-identifier mydbinstance
```

```
2009-12-22T23:44:14.374Z mydbinstance Allocated storage has been exhausted db-instance
2009-12-23T00:14:02.737Z mydbinstance Applying modification to allocated storage db-
instance
2009-12-23T00:31:54.764Z mydbinstance Finished applying modification to allocated storage
```

Amazon RDS insufficient DB instance capacity

The `InsufficientDBInstanceCapacity` error can be returned when you try to create, start, or modify a DB instance. It can also be returned when you try to restore a DB instance from a DB snapshot. When this error is returned, a common cause is that the specific DB instance class isn't available in the requested Availability Zone. You can try one of the following to solve the problem:

- Retry the request with a different DB instance class.
- Retry the request with a different Availability Zone.
- Retry the request without specifying an explicit Availability Zone.

For information about troubleshooting instance capacity issues for Amazon EC2, see [Insufficient instance capacity](#) in the *Amazon EC2 User Guide*.

For information about modifying a DB instance, see [Modifying an Amazon RDS DB instance \(p. 327\)](#).

Freeable memory issues in Amazon RDS

Freeable memory is the total random access memory (RAM) on a DB instance that can be made available to the database engine. It's the sum of the free operating-system (OS) memory and the available buffer

and page cache memory. The database engine uses most of the memory on the host, but OS processes also use some RAM. Memory currently allocated to the database engine or used by OS processes isn't included in freeable memory. When the database engine is running out of memory, the DB instance can use the temporary space that is normally used for buffering and caching. As previously mentioned, this temporary space is included in freeable memory.

You use the `FreeableMemory` metric in Amazon CloudWatch to monitor the freeable memory. For more information, see [Overview of monitoring metrics in Amazon RDS \(p. 511\)](#).

If your DB instance consistently runs low on freeable memory or uses swap space, consider scaling up to a larger DB instance class. For more information, see [DB instance classes \(p. 10\)](#).

You can also change the memory settings. For example, on RDS for MySQL, you might adjust the size of the `innodb_buffer_pool_size` parameter. This parameter is set by default to 75 percent of physical memory. For more MySQL troubleshooting tips, see [How can I troubleshoot low freeable memory in an Amazon RDS for MySQL database?](#)

MySQL and MariaDB issues

You can diagnose and correct issues with MySQL and MariaDB DB instances.

Topics

- [Maximum MySQL and MariaDB connections \(p. 2147\)](#)
- [Diagnosing and resolving incompatible parameters status for a memory limit \(p. 2148\)](#)
- [Diagnosing and resolving lag between read replicas \(p. 2149\)](#)
- [Diagnosing and resolving a MySQL or MariaDB read replication failure \(p. 2150\)](#)
- [Creating triggers with binary logging enabled requires SUPER privilege \(p. 2151\)](#)
- [Diagnosing and resolving point-in-time restore failures \(p. 2152\)](#)
- [Replication stopped error \(p. 2153\)](#)
- [Read replica create fails or replication breaks with fatal error 1236 \(p. 2153\)](#)

Maximum MySQL and MariaDB connections

The maximum number of connections allowed to an RDS for MySQL or RDS for MariaDB DB instance is based on the amount of memory available for its DB instance class. A DB instance class with more memory available results in a larger number of connections available. For more information on DB instance classes, see [DB instance classes \(p. 10\)](#).

The connection limit for a DB instance is set by default to the maximum for the DB instance class. You can limit the number of concurrent connections to any value up to the maximum number of connections allowed. Use the `max_connections` parameter in the parameter group for the DB instance. For more information, see [Maximum number of database connections \(p. 2139\)](#) and [Working with parameter groups \(p. 289\)](#).

You can retrieve the maximum number of connections allowed for a MySQL or MariaDB DB instance by running the following query.

```
SELECT @@max_connections;
```

You can retrieve the number of active connections to a MySQL or MariaDB DB instance by running the following query.

```
SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

Diagnosing and resolving incompatible parameters status for a memory limit

A MariaDB or MySQL DB instance can be placed in **incompatible-parameters** status for a memory limit when both of the following conditions are met:

- The DB instance is either restarted at least three time in one hour or at least five times in one day, or an attempt to restart the DB instance fails.
- The potential memory usage of the DB instance exceeds 1.2 times the memory allocated to its DB instance class.

When a DB instance is restarted for the third time in one hour or for the fifth time in one day, Amazon RDS for MySQL performs a check for memory usage. The check makes the a calculation of the potential memory usage of the DB instance. The value returned by the calculation is the sum of the following values:

- **Value 1** – The sum of the following parameters:
 - innodb_additional_mem_pool_size
 - innodb_buffer_pool_size
 - innodb_log_buffer_size
 - key_buffer_size
 - query_cache_size (MySQL version 5.7 only)
 - tmp_table_size
- **Value 2** – The max_connections parameter multiplied by the sum of the following parameters:
 - binlog_cache_size
 - join_buffer_size
 - read_buffer_size
 - read_rnd_buffer_size
 - sort_buffer_size
 - thread_stack
- **Value 3** – If the performance_schema parameter is enabled, then multiply the max_connections parameter by 257700.

If the performance_schema parameter is disabled, then this value is zero.

So, the value returned by the calculation is the following:

Value 1 + Value 2 + Value 3

When this value exceeds 1.2 times the memory allocated to the DB instance class used by the DB instance, the DB instance is placed in **incompatible-parameters** status. For information about the memory allocated to DB instance classes, see [Hardware specifications for DB instance classes \(p. 55\)](#).

The calculation multiplies the value of the max_connections parameter by the sum of several parameters. If the max_connections parameter is set to a large value, it might cause the check to return an inordinately high value for the potential memory usage of the DB instance. In this case, consider lowering the value of the max_connections parameter.

To resolve the problem, complete the following steps:

1. Adjust the memory parameters in the DB parameter group associated with the DB instance. Do so such that the potential memory usage is lower than 1.2 times the memory allocated to its DB instance class.

For information about setting parameters, see [Modifying parameters in a DB parameter group \(p. 294\)](#).

2. Restart the DB instance.

For information about setting parameters, see [Starting an Amazon RDS DB instance that was previously stopped \(p. 320\)](#).

Diagnosing and resolving lag between read replicas

After you create a MySQL or MariaDB read replica and the replica is available, Amazon RDS first replicates the changes made to the source DB instance from the time the read replica create operation started. During this phase, the replication lag time for the read replica is greater than 0. You can monitor this lag time in Amazon CloudWatch by viewing the Amazon RDS ReplicaLag metric.

The ReplicaLag metric reports the value of the Seconds_Behind_Master field of the MariaDB or MySQL SHOW REPLICAS STATUS command. For more information, see [SHOW REPLICAS STATUS](#). When the ReplicaLag metric reaches 0, the replica has caught up to the source DB instance. If the ReplicaLag metric returns -1, replication might not be active. To troubleshoot a replication error, see [Diagnosing and resolving a MySQL or MariaDB read replication failure \(p. 2150\)](#). A ReplicaLag value of -1 can also mean that the Seconds_Behind_Master value can't be determined or is NULL.

Note

Previous versions of MariaDB and MySQL used SHOW SLAVE STATUS instead of SHOW REPLICAS STATUS. If you are using a MariaDB version before 10.5 or a MySQL version before 8.0.23, then use SHOW SLAVE STATUS.

The ReplicaLag metric returns -1 during a network outage or when a patch is applied during the maintenance window. In this case, wait for network connectivity to be restored or for the maintenance window to end before you check the ReplicaLag metric again.

The MySQL and MariaDB read replication technology is asynchronous. Thus, you can expect occasional increases for the BinLogDiskUsage metric on the source DB instance and for the ReplicaLag metric on the read replica. For example, consider a situation where a high volume of write operations to the source DB instance occur in parallel. At the same time, write operations to the read replica are serialized using a single I/O thread. Such a situation can lead to a lag between the source instance and read replica.

For more information about read replicas and MySQL, see [Replication implementation details in the MySQL documentation](#). For more information about read replicas and MariaDB, see [Replication overview in the MariaDB documentation](#).

You can reduce the lag between updates to a source DB instance and the subsequent updates to the read replica by doing the following:

- Set the DB instance class of the read replica to have a storage size comparable to that of the source DB instance.
- Make sure that parameter settings in the DB parameter groups used by the source DB instance and the read replica are compatible. For more information and an example, see the discussion of the max_allowed_packet parameter in the next section.
- Disable the query cache. For tables that are modified often, using the query cache can increase replica lag because the cache is locked and refreshed often. If this is the case, you might see less replica lag if you disable the query cache. You can disable the query cache by setting the query_cache_type parameter to 0 in the DB parameter group for the DB instance. For more information on the query cache, see [Query cache configuration](#).

- Warm the buffer pool on the read replica for InnoDB for MySQL or MariaDB. For example, suppose that you have a small set of tables that are being updated often and you're using the InnoDB or XtraDB table schema. In this case, dump those tables on the read replica. Doing this causes the database engine to scan through the rows of those tables from the disk and then cache them in the buffer pool. This approach can reduce replica lag. The following shows an example.

For Linux, macOS, or Unix:

```
PROMPT> mysqldump \
-h <endpoint> \
--port=<port> \
-u=<username> \
-p <password> \
database_name table1 table2 > /dev/null
```

For Windows:

```
PROMPT> mysqldump ^
-h <endpoint> ^
--port=<port> ^
-u=<username> ^
-p <password> ^
database_name table1 table2 > /dev/null
```

Diagnosing and resolving a MySQL or MariaDB read replication failure

Amazon RDS monitors the replication status of your read replicas. RDS updates the **Replication State** field of the read replica instance to **Error** if replication stops for any reason. You can review the details of the associated error thrown by the MySQL or MariaDB engines by viewing the **Replication Error** field. Events that indicate the status of the read replica are also generated, including [RDS-EVENT-0045 \(p. 675\)](#), [RDS-EVENT-0046 \(p. 675\)](#), and [RDS-EVENT-0047 \(p. 672\)](#). For more information about events and subscribing to events, see [Working with Amazon RDS event notification \(p. 650\)](#). If a MySQL error message is returned, check the error in the [MySQL error message documentation](#). If a MariaDB error message is returned, check the error in the [MariaDB error message documentation](#).

Common situations that can cause replication errors include the following:

- The value for the `max_allowed_packet` parameter for a read replica is less than the `max_allowed_packet` parameter for the source DB instance.

The `max_allowed_packet` parameter is a custom parameter that you can set in a DB parameter group. The `max_allowed_packet` parameter is used to specify the maximum size of data manipulation language (DML) that can be run on the database. In some cases, the `max_allowed_packet` value for the source DB instance might be larger than the `max_allowed_packet` value for the read replica. If so, the replication process can throw an error and stop replication. The most common error is `packet bigger than 'max_allowed_packet'` bytes. You can fix the error by having the source and read replica use DB parameter groups with the same `max_allowed_packet` parameter values.

- Writing to tables on a read replica. If you're creating indexes on a read replica, you need to have the `read_only` parameter set to `0` to create the indexes. If you're writing to tables on the read replica, it can break replication.
- Using a nontransactional storage engine such as MyISAM. Read replicas require a transactional storage engine. Replication is only supported for the following storage engines: InnoDB for MySQL or MariaDB.

You can convert a MyISAM table to InnoDB with the following command:

```
alter table <schema>.<table_name> engine=innodb;
```

- Using unsafe nondeterministic queries such as SYSDATE(). For more information, see [Determination of safe and unsafe statements in binary logging](#) in the MySQL documentation.

The following steps can help resolve your replication error:

- If you encounter a logical error and you can safely skip the error, follow the steps described in [Skipping the current replication error \(p. 1428\)](#). Your MySQL or MariaDB DB instance must be running a version that includes the mysql_rds_skip_repl_error procedure. For more information, see [mysql.rds_skip_repl_error \(p. 1455\)](#).
- If you encounter a binary log (binlog) position issue, you can change the replica replay position with the mysql_rds_next_master_log command. Your MySQL or MariaDB DB instance must be running a version that supports the mysql_rds_next_master_log command to change the replica replay position. For version information, see [mysql.rds_next_master_log \(p. 1456\)](#).
- You might encounter a temporary performance issue due to high DML load. If so, you can set the innodb_flush_log_at_trx_commit parameter to 2 in the DB parameter group on the read replica. Doing this can help the read replica catch up, though it temporarily reduces atomicity, consistency, isolation, and durability (ACID).
- You can delete the read replica and create an instance using the same DB instance identifier. If you do this, the endpoint remains the same as that of your old read replica.

If a replication error is fixed, the **Replication State** changes to **replicating**. For more information, see [Troubleshooting a MySQL read replica problem \(p. 1399\)](#).

Creating triggers with binary logging enabled requires SUPER privilege

When trying to create triggers in an RDS for MySQL or RDS for MariaDB DB instance, you might receive the following error.

```
"You do not have the SUPER privilege and binary logging is enabled"
```

To use triggers when binary logging is enabled requires the SUPER privilege, which is restricted for RDS for MySQL and RDS for MariaDB DB instances. You can create triggers when binary logging is enabled without the SUPER privilege by setting the log_bin_trust_function_creators parameter to true. To set the log_bin_trust_function_creators to true, create a new DB parameter group or modify an existing DB parameter group.

You can create a new DB parameter group so you can create triggers in your RDS for MySQL or RDS for MariaDB DB instance with binary logging enabled. To do so, use the following CLI commands. To modify an existing parameter group, start with step 2.

To create a new parameter group to allow triggers with binary logging enabled using the CLI

1. Create a new parameter group.

For Linux, macOS, or Unix:

```
aws rds create-db-parameter-group \
--db-parameter-group-name allow-triggers \
--db-parameter-group-family mysql8.0 \
```

```
--description "parameter group allowing triggers"
```

For Windows:

```
aws rds create-db-parameter-group ^
--db-parameter-group-name allow-triggers ^
--db-parameter-group-family mysql8.0 ^
--description "parameter group allowing triggers"
```

2. Modify the DB parameter group to allow triggers.

For Linux, macOS, or Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name allow-triggers \
--parameters "ParameterName=log_bin_trust_function_creators, ParameterValue=true,
ApplyMethod=pending-reboot"
```

For Windows:

```
aws rds modify-db-parameter-group ^
--db-parameter-group-name allow-triggers ^
--parameters "ParameterName=log_bin_trust_function_creators, ParameterValue=true,
ApplyMethod=pending-reboot"
```

3. Modify your DB instance to use the new DB parameter group.

For Linux, macOS, or Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--db-parameter-group-name allow-triggers \
--apply-immediately
```

For Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--db-parameter-group-name allow-triggers ^
--apply-immediately
```

4. For the changes to take effect, manually reboot the DB instance.

```
aws rds reboot-db-instance --db-instance-identifier mydbinstance
```

Diagnosing and resolving point-in-time restore failures

Restoring a DB Instance That Includes Temporary Tables

When attempting a point-in-time restore (PITR) of your MySQL or MariaDB DB instance, you might encounter the following error.

```
Database instance could not be restored because there has been incompatible database activity for restore
```

functionality. Common examples of incompatible activity include using temporary tables, in-memory tables, or using MyISAM tables. In this case, use of Temporary table was detected.

PITR relies on both backup snapshots and binary logs (binlogs) from MySQL or MariaDB to restore your DB instance to a particular time. Temporary table information can be unreliable in binlogs and can cause a PITR failure. If you use temporary tables in your MySQL or MariaDB DB instance, you can lower the possibility of a PITR failure. To do so, perform more frequent backups. A PITR failure is most probable in the time between a temporary table's creation and the next backup snapshot.

Restoring a DB Instance That Includes In-Memory Tables

You might encounter a problem when restoring a database that has in-memory tables. In-memory tables are purged during a restart. As a result, your in-memory tables might be empty after a reboot. We recommend that when you use in-memory tables, you architect your solution to handle empty tables in the event of a restart. If you're using in-memory tables with replicated DB instances, you might need to recreate the read replicas after a restart. This might be necessary if a read replica reboots and can't restore data from an empty in-memory table.

For more information about backups and PITR, see [Working with backups \(p. 427\)](#) and [Restoring a DB instance to a specified time \(p. 499\)](#).

Replication stopped error

When you call the `mysql.rds_skip_repl_error` command, you might receive an error message stating that replication is down or disabled.

This error message appears because replication is stopped and can't be restarted.

If you need to skip a large number of errors, the replication lag can increase beyond the default retention period for binary log files. In this case, you might encounter a fatal error due to binary log files being purged before they have been replayed on the replica. This purge causes replication to stop, and you can no longer call the `mysql.rds_skip_repl_error` command to skip replication errors.

You can mitigate this issue by increasing the number of hours that binary log files are retained on your replication source. After you have increased the binlog retention time, you can restart replication and call the `mysql.rds_skip_repl_error` command as needed.

To set the binlog retention time, use the [mysql.rds_set_configuration \(p. 1459\)](#) procedure. Specify a configuration parameter of 'binlog retention hours' along with the number of hours to retain binlog files on the DB cluster, up to 720 (30 days). The following example sets the retention period for binlog files to 48 hours.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

Read replica create fails or replication breaks with fatal error 1236

After changing default parameter values for a MySQL or MariaDB DB instance, you might encounter one of the following problems:

- You can't create a read replica for the DB instance.
- Replication fails with fatal error 1236.

Some default parameter values for MySQL and MariaDB DB instances help to make sure that the database is ACID compliant and read replicas are crash-safe. They do this by making sure that each

commit is fully synchronized by writing the transaction to the binary log before it's committed. Changing these parameters from their default values to improve performance can cause replication to fail when a transaction hasn't been written to the binary log.

To resolve this issue, set the following parameter values:

- `sync_binlog = 1`
- `innodb_support_xa = 1`
- `innodb_flush_log_at_trx_commit = 1`

Can't set backup retention period to 0

There are several reasons why you might need to set the backup retention period to 0. For example, you can disable automatic backups immediately by setting the retention period to 0.

In some cases, you might set the value to 0 and receive a message saying that the retention period must be between 1 and 35. In these cases, check to make sure that you haven't set up a read replica for the instance. Read replicas require backups for managing read replica logs, and therefore you can't set a retention period of 0.

Amazon RDS API reference

In addition to the AWS Management Console and the AWS Command Line Interface (AWS CLI), Amazon RDS also provides an API. You can use the API to automate tasks for managing your DB instances and other objects in Amazon RDS.

- For an alphabetical list of API operations, see [Actions](#).
- For an alphabetical list of data types, see [Data types](#).
- For a list of common query parameters, see [Common parameters](#).
- For descriptions of the error codes, see [Common errors](#).

For more information about the AWS CLI, see [AWS Command Line Interface reference for Amazon RDS](#).

Topics

- [Using the Query API \(p. 2155\)](#)
- [Troubleshooting applications on Amazon RDS \(p. 2155\)](#)

Using the Query API

The following sections briefly discuss the parameters and request authentication used with the Query API.

For general information about how the Query API works, see [Query requests](#) in the *Amazon EC2 API Reference*.

Query parameters

HTTP Query-based requests are HTTP requests that use the HTTP verb GET or POST and a Query parameter named Action.

Each Query request must include some common parameters to handle authentication and selection of an action.

Some operations take lists of parameters. These lists are specified using the `param.n` notation. Values of *n* are integers starting from 1.

For information about Amazon RDS Regions and endpoints, go to [Amazon Relational Database Service \(RDS\)](#) in the Regions and Endpoints section of the *Amazon Web Services General Reference*.

Query request authentication

You can only send Query requests over HTTPS, and you must include a signature in every Query request. You must use either AWS signature version 4 or signature version 2. For more information, see [Signature Version 4 signing process](#) and [Signature version 2 signing process](#).

Troubleshooting applications on Amazon RDS

Amazon RDS provides specific and descriptive errors to help you troubleshoot problems while interacting with the Amazon RDS API.

Topics

- [Retrieving errors \(p. 2156\)](#)
- [Troubleshooting tips \(p. 2156\)](#)

For information about troubleshooting for Amazon RDS DB instances, see [Troubleshooting for Amazon RDS \(p. 2141\)](#).

Retrieving errors

Typically, you want your application to check whether a request generated an error before you spend any time processing results. The easiest way to find out if an error occurred is to look for an `Error` node in the response from the Amazon RDS API.

XPath syntax provides a simple way to search for the presence of an `Error` node. It also provides a relatively easy way to retrieve the error code and message. The following code snippet uses Perl and the `XML::XPath` module to determine if an error occurred during a request. If an error occurred, the code prints the first error code and message in the response.

```
use XML::XPath;
my $xp = XML::XPath->new(xml =>$response);
if ( $xp->find("//Error") )
{print "There was an error processing your request:\n", " Error code: ",
$xp->findvalue("//Error[1]/Code"), "\n", " ",
$xp->findvalue("//Error[1]/Message"), "\n\n"; }
```

Troubleshooting tips

We recommend the following processes to diagnose and resolve problems with the Amazon RDS API:

- Verify that Amazon RDS is operating normally in the AWS Region that you're targeting by checking <http://status.aws.amazon.com>.
- Check the structure of your request.

Each Amazon RDS operation has a reference page in the *Amazon RDS API Reference*. Double-check that you are using parameters correctly. For ideas about what might be wrong, look at the sample requests or user scenarios to see if those examples do similar operations.

- Check AWS re:Post.

Amazon RDS has a development community where you can search for solutions to problems others have experienced along the way. To view the topics, go to [AWS re:Post](#).

Document history

Current API version: 2014-10-31

The following table describes important changes in each release of the *Amazon RDS User Guide* after May 2018. For notification about updates to this documentation, you can subscribe to an RSS feed.

Note

You can filter new Amazon RDS features on the [What's New with Database?](#) page. For **Products**, choose **Amazon RDS**. Then search using keywords such as **RDS Proxy** or **Oracle 2022**.

Change	Description	Date
Amazon RDS is available in the Asia Pacific (Hyderabad) Region (p. 2157)	Amazon RDS is now available in the Asia Pacific (Hyderabad) Region. For more information, see Regions and Availability Zones .	November 22, 2022
RDS supports MariaDB 10.6.11, 10.5.18, 10.4.27, and 10.3.37 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.6.11, 10.5.18, 10.4.27, and 10.3.37. For more information, see MariaDB on Amazon RDS versions .	November 18, 2022
RDS Custom for Oracle supports setting nondefault installation parameters in a custom engine version (CEV) (p. 2157)	When you create a CEV, you can set nondefault values for the Oracle base, Oracle home, UNIX user name and ID, and UNIX group name and ID. In this way, you gain more control over the database installation on your RDS Custom for Oracle DB instance. For more information, see Preparing the CEV manifest .	November 18, 2022
Amazon RDS supports Oracle APEX version 22.1.v1 (p. 2157)	You can use APEX 22.1.v1 with all supported versions of Oracle Database. For more information, see Oracle Application Express .	November 18, 2022
RDS for SQL Server supports cross-Region read replicas (p. 2157)	You can now create a cross-Region read replica to enhance disaster recovery capability, reduce application read latency, and offload read workloads from the primary DB Instance. For more information, see Creating a read replica in a different AWS Region .	November 16, 2022
Amazon RDS is available in the Europe (Spain) Region (p. 2157)	Amazon RDS is now available in the Europe (Spain) Region. For more information, see Regions and Availability Zones .	November 16, 2022

RDS for SQL Server supports linked servers for Oracle database (p. 2157)	You can now create a linked server to access external Oracle databases to read data and execute SQL commands. For more information, see Linked Servers with Oracle OLEDB with RDS for SQL Server .	November 15, 2022
RDS Custom for Oracle supports Oracle Multitenant (p. 2157)	You can create an RDS Custom for Oracle DB instance as a container database (CDB). After creation, the CDB contains the CDB root, PDB seed, and one PDB. You can add more PDBs manually using Oracle SQL. For more information, see Overview of Amazon RDS Custom for Oracle architecture .	November 15, 2022
Amazon RDS for Oracle supports Amazon EFS integration (p. 2157)	If you add the EFS_INTEGRATION option to your option group, you can transfer files between your RDS for Oracle DB instance and an Amazon EFS file system. For more information, see Amazon EFS .	November 15, 2022
RDS supports MySQL 8.0.31 and 5.7.40 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.31 and 5.7.40. For more information, see MySQL on Amazon RDS versions .	November 10, 2022
Amazon RDS is available in the Europe (Zurich) Region (p. 2157)	Amazon RDS is now available in the Europe (Zurich) Region. For more information, see Regions and Availability Zones .	November 9, 2022
Access to transaction log backups is now available for RDS for SQL Server (p. 2157)	You can now view and copy database transaction log backups to an Amazon S3 bucket. For more information, see Access to transaction log backups .	November 7, 2022
Multi-AZ DB clusters supported in additional AWS Regions (p. 2157)	Multi-AZ DB clusters are now available in additional AWS Regions. For more information, see Multi-AZ DB clusters .	November 4, 2022

Amazon RDS supports gp3 storage (p. 2157)	You can now create Amazon RDS DB instances that use Amazon EBS General Purpose SSD (gp3) storage volumes, which let you customize storage performance independently of storage capacity. For more information, see General Purpose SSD storage .	November 4, 2022
Amazon RDS Custom for SQL Server supports Scale Storage. (p. 2157)	You can now modify storage of existing RDS Custom for SQL Server database instances without incurring any downtime. You can scale up storage size and switch storage types from a general purpose workload to an I/O intensive workload. For more information, see Working with Amazon RDS Custom .	October 31, 2022
Amazon RDS supports a new event for operating system updates (p. 2157)	Amazon RDS now supports a new DB instance event, RDS-EVENT-0230, under the event category of security patching. This new event alerts you when an operating system update is available for your DB instance. For more information, see Monitoring Amazon RDS events and Working with operating system updates .	October 28, 2022
Amazon RDS for Oracle supports preconfigured r5b memory optimized instance classes (p. 2157)	The r5b Oracle DB instance classes are optimized for workloads that require additional memory, storage, and I/O per vCPU. For example, db.r5b.4xlarge.tpc2.mem2x has multithreading turned on and provides twice as much memory as db.r5b.4xlarge. For more information, see RDS for Oracle instance classes .	October 27, 2022
Amazon RDS supports 15 read replicas for RDS for MariaDB, MySQL, and PostgreSQL DB instances (p. 2157)	You can now create up to 15 read replicas for RDS for MariaDB, MySQL, and PostgreSQL DB instances. For more information about read replicas, see Working with read replicas .	October 20, 2022

Amazon RDS for PostgreSQL now supports PostgreSQL version 15 RC 3 in the database preview environment (p. 2157)	PostgreSQL version 15 Beta 3 is now available in the database preview environment in the US East (Ohio) AWS Region. For more information, see Working with the database preview environment .	October 18, 2022
Amazon RDS supports automatically setting up connectivity between an RDS database and an EC2 instance (p. 2157)	You can use the AWS Management Console to set up connectivity between an existing RDS DB instance or Multi-AZ DB cluster and an EC2 instance. For more information, see Connecting an EC2 instance and an RDS database automatically .	October 14, 2022
AWS JDBC Driver for PostgreSQL generally available (p. 2157)	The AWS JDBC Driver for PostgreSQL is a client driver designed for RDS for PostgreSQL. The AWS JDBC Driver for PostgreSQL is now generally available. For more information, see Connecting with the AWS JDBC Driver for PostgreSQL .	October 6, 2022
Amazon RDS for Oracle supports Oracle APEX version 21.2.v1 (p. 2157)	APEX 21.2 includes patch 33420059. For more information, see APEX version requirements .	October 3, 2022
RDS supports MySQL 5.7.39 (p. 2157)	You can now create Amazon RDS DB instances running MySQL versions 5.7.39. For more information, see MySQL on Amazon RDS versions .	September 29, 2022
RDS supports MariaDB 10.6.10 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.6.10. For more information, see MariaDB on Amazon RDS versions .	September 29, 2022
RDS Proxy supports RDS for SQL Server (p. 2157)	You can now create an RDS Proxy for an RDS DB instance that runs Microsoft SQL Server version 2014 or higher. For more information about RDS Proxy, see Using Amazon RDS Proxy .	September 19, 2022
RDS supports MariaDB 10.5.17, 10.4.26, and 10.3.36 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.5.17, 10.4.26, and 10.3.36. For more information, see MariaDB on Amazon RDS versions .	September 15, 2022

Amazon RDS for Oracle supports local instance storage for temporary data (p. 2157)	You can now launch Amazon RDS for Oracle on Amazon EC2 db.r5d and db.m5d instance types with the temporary tablespace and Database Smart Flash Cache (the flash cache) configured to use an instance store. By storing temporary data locally, you can achieve lower read and write latencies when compared to standard storage based on Amazon EBS. For more information, see Storing temporary Oracle data in the instance store .	September 14, 2022
Performance Insights shows the top 25 SQL queries (p. 2157)	In the Performance Insights dashboard, the Top SQL tab shows the 25 SQL queries that are contributing the most to DB load. For more information, see Overview of the Top SQL tab .	September 13, 2022
RDS supports MySQL 8.0.30 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.30. For more information, see MySQL on Amazon RDS versions .	September 9, 2022
Amazon RDS is available in the Middle East (UAE) Region (p. 2157)	Amazon RDS is now available in the Middle East (UAE) Region. For more information, see Regions and Availability Zones .	August 30, 2022
Amazon RDS for SQL Server supports SSRS Email subscriptions (p. 2157)	You can now use the SQL Server Reporting Services (SSRS) Email extension to send reports to users and subscribe to reports on the report server. For more information, see Support for SQL Server Reporting Services in RDS for SQL Server .	August 26, 2022
RDS for Oracle supports read replica backups (p. 2157)	You can turn on automatic backups and create manual snapshots of RDS for Oracle replicas. For more information, see Working with RDS for Oracle replica backups .	August 23, 2022

RDS for Oracle supports Oracle Data Guard switchover (p. 2157)	A switchover is a role reversal between a primary database and a mounted or open Oracle replica. During a switchover, the original primary database transitions to a standby role, while the original standby database transitions to the primary role. For more information, see Performing an Oracle Data Guard switchover .	August 23, 2022
Amazon RDS supports automatically setting up connectivity with an EC2 instance (p. 2157)	When you create a DB instance or Multi-AZ DB cluster, you can use the AWS Management Console to set up connectivity between an Amazon Elastic Compute Cloud instance and the new DB instance or DB cluster. For more information, see Configure automatic network connectivity with an EC2 instance for a new DB instance and Configure automatic network connectivity with an EC2 instance for a new DB cluster.	August 22, 2022
RDS Custom for Oracle supports promotion of Oracle replicas (p. 2157)	If you use RDS Custom for Oracle, you can promote your managed Oracle replicas by using the <code>promote-read-replica</code> CLI command. Also, you can delete your primary DB instance, which causes RDS Custom for Oracle to promote your managed Oracle replicas to standalone instances. For more information, see Working with Oracle replicas for RDS Custom for Oracle .	August 5, 2022
RDS for MySQL supports enforcing SSL/TLS connections (p. 2157)	RDS for MySQL now supports enforcing SSL/TLS connections by setting the <code>require_secure_transport</code> parameter to ON. For more information, see Requiring an SSL/TLS connection to a MySQL DB instance .	August 1, 2022

Amazon RDS has deprecated support for Oracle Database 12c Release 1 (12.1.0.2) (p. 2157)	Support for version 12.1.0.2 is deprecated for both the BYOL and LI licensing models. On August 1, 2022, RDS for Oracle begins automatic upgrades of 12c Release 1 (12.1.0.2) DB instances and restored 12.1.0.2 snapshots to Oracle Database 19c. For more information, see Oracle Database 12c with Amazon RDS and the end of support timeline on AWS re:Post .	August 1, 2022
RDS Proxy supports RDS for MariaDB (p. 2157)	You can now create an RDS Proxy for an RDS DB instance that runs MariaDB version 10.2, 10.3, 10.4, or 10.5. The MariaDB support is included under the MySQL engine family. For more information about RDS Proxy, see Using Amazon RDS Proxy .	July 26, 2022
RDS for MariaDB supports the db.r5b DB instance classes (p. 2157)	You can now create RDS for MariaDB DB instances that use the db.r5b DB instance classes. For more information, Supported DB engines for DB instance classes .	July 25, 2022
RDS for Oracle supports modifying database activity streams (p. 2157)	If you use RDS for Oracle, you can change the audit policy state of a database activity stream to either locked (default) or unlocked. Instead of stopping an activity stream, you can unlock its policy state, customize your audit policy, and then relock the policy state. For more information, see Modifying a database activity stream .	July 22, 2022
Performance Insights supports the Asia Pacific (Jakarta) Region (p. 2157)	Formerly, you couldn't use Performance Insights in the Asia Pacific (Jakarta) Region. This restriction has been removed. For more information, see AWS Region support for Performance Insights .	July 21, 2022

Microsoft SQL Server 2012 has reached its end of support on Amazon RDS (p. 2157)	Microsoft SQL Server 2012 has reached its end of support, coinciding with the Microsoft plan to end extended support for this version on July 12, 2022. Any existing Microsoft SQL Server 2012 instances are to be automatically upgraded to the latest minor version of Microsoft SQL Server 2014 starting on June 1, 2022. For more information, see Microsoft SQL Server 2012 support on Amazon RDS .	July 12, 2022
RDS supports MariaDB 10.6.8, 10.5.16, 10.4.25, 10.3.35, and 10.2.44 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.6.8, 10.5.16, 10.4.25, 10.3.35, and 10.2.44. For more information, see Supported MariaDB versions on Amazon RDS .	July 8, 2022
RDS Performance Insights supports additional retention periods (p. 2157)	Previously, Performance Insights offered only two retention periods: 7 days (default) or 2 years (731 days). Now, if you need to retain your performance data for longer than 7 days, you can specify from 1–24 months. For more information, see Pricing and data retention for Performance Insights .	July 1, 2022
RDS Custom supports the Asia Pacific (Mumbai) and Europe (London) Regions (p. 2157)	You can create RDS Custom for Oracle and RDS Custom for SQL Server DB instances in two new AWS Regions: Asia Pacific (Mumbai) and Europe (London). For more information, see AWS Region support for RDS Custom for Oracle and AWS Region support for RDS Custom for SQL Server .	June 21, 2022
RDS Custom for Oracle supports Oracle Database 18c and 12c Release 2 (12.2) (p. 2157)	You can now create a CEV for RDS Custom for Oracle using installation files for Oracle Database 18c and 12c Release 2 (12.2). You can use these CEVs to create an RDS Custom for Oracle DB instance. For more information, see Working with custom engine versions for Amazon RDS Custom for Oracle .	June 21, 2022

Multi-AZ DB clusters support the db.m5d and db.r5d DB instance classes (p. 2157)	You can now create Multi-AZ DB clusters that use the db.m5d and db.r5d DB instance classes. For more information, see Multi-AZ DB cluster deployments and DB instance class types .	June 21, 2022
Multi-AZ DB clusters available in additional AWS Regions (p. 2157)	You can now create Multi-AZ DB clusters in the following Regions: Europe (Frankfurt) and Europe (Stockholm). For more information, see Multi-AZ DB cluster deployments .	June 21, 2022
RDS for Microsoft SQL Server supports migration of databases that use Transparent Data Encryption (TDE) (p. 2157)	RDS for SQL Server now supports migrating Microsoft SQL Server databases with TDE turned on, using native backup and restore. For more information, see Support for Transparent Data Encryption in SQL Server .	June 14, 2022
Amazon RDS supports publishing events to encrypted Amazon SNS topics (p. 2157)	Amazon RDS can now publish events to Amazon Simple Notification Service (Amazon SNS) topics that have server-side encryption (SSE) enabled, for additional protection of events that carry sensitive data. For more information, see Subscribing to Amazon RDS event notification .	June 1, 2022
RDS supports MySQL 5.7.38 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.38. For more information, see MySQL on Amazon RDS versions .	May 31, 2022
RDS for PostgreSQL supports cascading read replicas (p. 2157)	You can now use cascading read replicas with RDS for PostgreSQL version 14.1 and higher releases. For more information, see Working with PostgreSQL read replicas in Amazon RDS .	May 4, 2022
Amazon RDS on AWS Outposts supports scale storage and autoscaling operations (p. 2157)	You can now change the storage sizes of DB instances on your Outpost and use storage autoscaling. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	May 2, 2022

Multi-AZ DB clusters available in additional AWS Regions (p. 2157)	You can now create Multi-AZ DB clusters in the following Regions: Asia Pacific (Singapore) and Asia Pacific (Sydney). For more information, see Multi-AZ DB cluster deployments .	April 29, 2022
Amazon RDS supports dual-stack mode (p. 2157)	DB instances can now run in dual-stack mode. In dual-stack mode, resources can communicate with the DB instance over IPv4, IPv6, or both. For more information, see Amazon RDS IP addressing .	April 29, 2022
Amazon RDS publishes usage metrics to Amazon CloudWatch (p. 2157)	The AWS/Usage namespace in Amazon CloudWatch includes account-level usage metrics for your Amazon RDS service quotas. For more information, see Amazon CloudWatch usage metrics for Amazon RDS .	April 28, 2022
Amazon RDS for MySQL supports the db.m6i and db.r6i DB instance classes (p. 2157)	You can now use the db.m6i and db.r6i DB instance classes for Amazon RDS DB instances running MySQL. For more information, see Supported DB engines for DB instance classes .	April 28, 2022
Amazon RDS for PostgreSQL supports the db.m6i and db.r6i DB instance classes (p. 2157)	You can now use the db.m6i and db.r6i DB instance classes for Amazon RDS DB instances running PostgreSQL. For more information, see Supported DB engines for DB instance classes .	April 27, 2022
Amazon RDS for MariaDB supports the db.m6i and db.r6i DB instance classes (p. 2157)	You can now use the db.m6i and db.r6i DB instance classes for Amazon RDS DB instances running MariaDB. For more information, see Supported DB engines for DB instance classes .	April 26, 2022
Amazon RDS on AWS Outposts supports Multi-AZ deployments (p. 2157)	You can now create a standby DB instance on a different Outpost. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	April 19, 2022

Amazon RDS for Oracle supports the db.m6i and db.r6i instance classes (p. 2157)	If you run Oracle Database 19c, you can use the db.m6i and db.r6i instance classes. The db.m6i classes are general-purpose instance classes that are well suited for a broad range of workloads. For more information, see RDS for Oracle instance classes .	April 8, 2022
Amazon RDS for SQL Server supports SQL Server Agent job replication (p. 2157)	When you turn on this feature, SQL Server Agent jobs created, modified, or deleted on the primary host are automatically synchronized to the secondary host in a Multi-AZ configuration. For more information, see Using SQL Server Agent .	April 7, 2022
Amazon RDS supports RDS Proxy with RDS for PostgreSQL version 13 (p. 2157)	You can now create an RDS Proxy with an RDS for PostgreSQL version 13 database. For more information about RDS Proxy, see Using Amazon RDS Proxy .	April 4, 2022
Amazon RDS plans to deprecate Oracle Database 12c (p. 2157)	Oracle Database 12c is on a deprecation path. Oracle Corporation will no longer provide patches for Oracle Database 12c releases after the end-of-support dates. Amazon RDS plans to begin automatically upgrading Oracle Database 12c DB instances to Oracle Database 19c. For more information, see Oracle Database 12c with Amazon RDS and Preparing for the automatic upgrade of Oracle Database 12c .	March 22, 2022
Amazon RDS for PostgreSQL Release Notes (p. 2157)	There is now a separate guide for the Amazon RDS for PostgreSQL release notes. For more information, see Amazon RDS for PostgreSQL Release Notes .	March 22, 2022
Amazon RDS for Oracle Release Notes (p. 2157)	There is now a separate guide for the Amazon RDS for Oracle release notes. For more information, see Amazon RDS for Oracle Release Notes .	March 22, 2022

Multi-AZ DB clusters available in additional AWS Regions (p. 2157)	You can now create Multi-AZ DB clusters in the following Regions: US East (Ohio) and Asia Pacific (Tokyo). For more information, see Multi-AZ DB cluster deployments .	March 15, 2022
Amazon RDS for PostgreSQL versions 14.2, 13.6, 12.10, 11.15, and 10.20 (p. 2157)	RDS for PostgreSQL now supports versions 14.2, 13.6, 12.10, 11.15, and 10.20. Version 14.2 and 13.6 add support for two new foreign data wrappers. The mysql_fdw extension lets PostgreSQL work with data stored in MySQL, MariaDB, and Aurora MySQL databases. The tds_fdw extension lets PostgreSQL work with data stored in SQL Server databases. For more information, see Supported PostgreSQL database versions .	March 12, 2022
RDS supports MySQL 5.7.37 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.37. For more information, see MySQL on Amazon RDS versions .	March 11, 2022
Amazon RDS for SQL Server supports new DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running Microsoft SQL Server that use the db.m6i and db.r6i DB instance classes. For more information, see DB instance class support for Microsoft SQL Server .	March 9, 2022
Amazon RDS for Oracle supports Oracle Database 21c (p. 2157)	You can now create Amazon RDS DB instances running Oracle Database 21c (21.0.0.0). This is the first Oracle Database release that supports only the multitenant (CDB) architecture. For more information, see Oracle Database 21c with Amazon RDS .	March 7, 2022
RDS supports MariaDB 10.6.7, 10.5.15, 10.4.24, 10.3.34, and 10.2.43 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.6.7, 10.5.15, 10.4.24, 10.3.34, and 10.2.43. For more information, see MariaDB on Amazon RDS versions .	March 3, 2022

AWS JDBC Driver for MySQL generally available (p. 2157)	The AWS JDBC Driver for MySQL is a client driver designed for RDS for MySQL. The AWS JDBC Driver for MySQL is now generally available. For more information, see Connecting with the Amazon Web Services JDBC Driver for MySQL .	March 2, 2022
Multi-AZ DB clusters generally available (p. 2157)	A Multi-AZ DB cluster deployment is a high availability deployment mode of Amazon RDS with two readable standby DB instances. Multi-AZ DB clusters are now generally available. For more information, see Multi-AZ DB cluster deployments .	March 1, 2022
RDS supports MySQL 8.0.28 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.28. For more information, see MySQL on Amazon RDS versions .	February 28, 2022
Amazon RDS for Oracle supports new settings for native network encryption (NNE) (p. 2157)	To control whether clients can connect with non-secure encryption and checksumming methods, set SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS and SQLNET.ALLOW_WEAK_CRYPTO in the NNE option. Examples of insecure methods include DES, 3DES, RC4, and MD5. For more information, see NNE option settings .	February 25, 2022
Amazon RDS for SQL Server supports Always On Availability Groups for Microsoft SQL Server 2017 Standard Edition (p. 2157)	When you create a DB instance using the Multi-AZ configuration on SQL Server 2017 Standard Edition 14.00.3401.7 and higher versions, RDS automatically uses Availability Groups. For more information, see Multi-AZ deployments for Microsoft SQL Server .	February 18, 2022
RDS for Oracle supports Database Activity Streams in the Asia Pacific (Jakarta) Region (p. 2157)	For more information, see Support for AWS Regions for database activity streams .	February 16, 2022

Amazon RDS Custom for Oracle support for Oracle Database 12.1 (p. 2157)	You can now create custom engine versions for RDS Custom for Oracle that use Oracle Database 12.1 Enterprise Edition. For more information, see Working with custom engine versions for Amazon RDS Custom for Oracle .	February 4, 2022
Amazon RDS for MariaDB supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.6. For more information, see MariaDB 10.6 support on Amazon RDS .	February 3, 2022
Performance Insights supports plan capture for Oracle queries (p. 2157)	The Performance Insights console supports a new plan dimension for top SQL. When you slice by plan, you can see which plans your top Oracle queries are using. If a query uses multiple plans, you can compare the plans side by side in the console and determine which plan is most efficient. You can also drill down to see which steps in a plan have the highest cost. For more information, see Analyzing Oracle execution plans using the Performance Insights dashboard .	January 27, 2022
Performance Insights supports new APIs (p. 2157)	Performance Insights supports the following APIs: <code>GetResourceMetadata</code> , <code>ListAvailableResourceDimensions</code> , and <code>ListAvailableResourceMetrics</code> . For more information, see Retrieving metrics with the Performance Insights API in this manual and the Amazon RDS Performance Insights API Reference .	January 12, 2022
RDS Proxy supports events (p. 2157)	RDS Proxy now generates events that you can subscribe to and view in CloudWatch Events or configure to send to Amazon EventBridge. For more information, see Working with RDS Proxy events .	January 11, 2022

Amazon RDS for SQL Server supports SSAS Multidimensional mode (p. 2157)	RDS for SQL Server supports running SQL Server Analysis Services (SSAS) in Tabular or Multidimensional mode. For more information, see Support for SQL Server Analysis Services in RDS for SQL Server .	January 7, 2022
RDS Proxy available in additional AWS Regions (p. 2157)	RDS Proxy is now available in the following Regions: Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Osaka), Europe (Milan), Europe (Paris), Europe (Stockholm), Middle East (Bahrain), and South America (São Paulo). For more information about RDS Proxy, see Using Amazon RDS Proxy .	January 5, 2022
RDS supports MySQL 8.0.27 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.27. For more information, see MySQL on Amazon RDS versions .	December 21, 2021
Amazon RDS is available in the Asia Pacific (Jakarta) Region (p. 2157)	Amazon RDS is now available in the Asia Pacific (Jakarta) Region. For more information, see Regions and Availability Zones .	December 13, 2021
Amazon RDS supports MariaDB 10.5.13, 10.4.22, 10.3.32, and 10.2.41 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.5.13, 10.4.22, 10.3.32, and 10.2.41. For more information, see MariaDB on Amazon RDS versions .	December 8, 2021
Amazon RDS Custom for SQL Server (p. 2157)	Amazon RDS Custom is a managed database service for legacy, custom, and packaged applications that require access to the underlying operating system and database environment. With Amazon RDS Custom, you get the automation of Amazon RDS and the flexibility of Amazon EC2. For more information, see Working with Amazon RDS Custom .	December 1, 2021

Multi-AZ DB clusters (preview) (p. 2157)	You can now create Multi-AZ DB clusters for RDS for MySQL and RDS for PostgreSQL. A Multi-AZ DB cluster deployment is a high availability deployment mode of Amazon RDS with two readable standby DB instances. Multi-AZ DB clusters are in preview. For more information, see Multi-AZ DB cluster deployments (preview) .	November 23, 2021
Amazon RDS supports RDS Proxy with RDS for PostgreSQL version 12 (p. 2157)	You can now create an RDS Proxy with an RDS for PostgreSQL version 12 database. For more information about RDS Proxy, see Using Amazon RDS Proxy .	November 22, 2021
Amazon RDS on AWS Outposts supports local backups (p. 2157)	You can store automated backups and manual snapshots in your AWS Region or locally on your Outpost. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	November 22, 2021
Amazon RDS support for cross-account AWS KMS keys (p. 2157)	You can use a KMS key from a different AWS account for encryption when exporting DB snapshots to Amazon S3. For more information, see Exporting DB snapshot data to Amazon S3 .	November 3, 2021
Amazon RDS on AWS Outposts supports publishing database engine logs to CloudWatch Logs (p. 2157)	RDS on Outposts now supports publishing database engine logs to CloudWatch Logs. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	November 2, 2021
Amazon RDS Custom for Oracle (p. 2157)	Amazon RDS Custom is a managed database service for legacy, custom, and packaged applications that require access to the underlying operating system and database environment. With Amazon RDS Custom, you get the automation of Amazon RDS and the flexibility of Amazon EC2. For more information, see Working with Amazon RDS Custom .	October 26, 2021

Support for delayed replication for RDS for MySQL version 8.0 (p. 2157)	Starting with RDS for MySQL version 8.0.26, you can configure delayed replication for RDS for MySQL version 8.0 DB instances. For more information, see Configuring delayed replication with MySQL .	October 25, 2021
Support for MySQL 8.0.26 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.26. For more information, see MySQL on Amazon RDS versions .	October 25, 2021
Support for GTID-based replication for RDS for MySQL version 8.0 (p. 2157)	Starting with RDS for MySQL version 8.0.26, you can configure GTID-based replication for RDS for MySQL version 8.0 DB instances. For more information, see Using GTID-based replication for RDS for MySQL .	October 25, 2021
Amazon RDS supports RDS Proxy with RDS for MySQL 8.0 (p. 2157)	You can now create an RDS Proxy for an RDS for MySQL 8.0 database instance. For more information, see Using Amazon RDS Proxy .	October 21, 2021
Amazon RDS on AWS Outposts supports additional RDS for MySQL versions (p. 2157)	RDS on Outposts now supports RDS for MySQL versions 8.0.23 and 8.0.25. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	October 20, 2021
Amazon RDS for PostgreSQL now supports PostgreSQL version 14 RC 1 in the database preview environment (p. 2157)	PostgreSQL version 14 RC 1 is now available in the database preview environment in the US East (Ohio) AWS Region. For more information, see Working with the database preview environment .	October 19, 2021
Amazon RDS supports Performance Insights in additional AWS Regions (p. 2157)	Performance Insights is available in the Middle East (Bahrain), Africa (Cape Town), Europe (Milan), and Asia Pacific (Osaka) Regions. For more information, see AWS Region support for Performance Insights .	October 5, 2021
Performance Insights supports digest-level statistics for Oracle (p. 2157)	When you use Performance Insights, you can view SQL statistics both at the statement and digest level for Amazon RDS for Oracle. For more information, see Analyzing running queries in Oracle .	October 4, 2021

Amazon RDS on AWS Outposts supports additional RDS for PostgreSQL versions (p. 2157)	RDS on Outposts now supports RDS for PostgreSQL versions 12.8 and 13.4. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	October 1, 2021
Amazon RDS supports Oracle APEX version 21.1.v1 (p. 2157)	You can use APEX 21.1.v1 with all supported versions of Oracle Database. For more information, see Oracle Application Express .	September 24, 2021
Amazon RDS for Oracle supports client-side encryption for NNE (p. 2157)	When you configure NNE, you might want to avoid forcing encryption on the server side. For example, you might not want to force all client communications to use encryption because the server requires it. In this case, you can force encryption on the client side using the SQLNET.*CLIENT options. For more information, see Oracle native network encryption .	September 24, 2021
Amazon RDS for MySQL and RDS for PostgreSQL support new DB instance classes (p. 2157)	You can now use the db.r5b, db.t4g, and db.x2g instance classes to create Amazon RDS DB instances running MySQL or PostgreSQL. For more information, see Supported DB engines for DB instance classes .	September 15, 2021
Amazon RDS for Microsoft SQL Server supports Java Database Connectivity (JDBC) with Microsoft Distributed Transaction Coordinator (MSDTC) (p. 2157)	JDBC XA transactions are now supported with MSDTC for SQL Server 2017 version 14.00.3223.3 and higher, and SQL Server 2019. For more information, see Support for Microsoft Distributed Transaction Coordinator in RDS for SQL Server .	September 7, 2021
Amazon RDS supports MariaDB 10.5.12, 10.4.21, 10.3.31, and 10.2.40 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.5.12, 10.4.21, 10.3.31, and 10.2.40. For more information, see MariaDB on Amazon RDS versions .	September 2, 2021

Amazon RDS has ended support for Oracle Database 18c (p. 2157)	You can create DB instances only for Oracle Database 12c and Oracle Database 19c. If you have Oracle Database 18c snapshots, upgrade them to a later release. For more information, see Upgrading an Oracle DB snapshot .	August 17, 2021
Amazon RDS for SQL Server supports automatic minor version upgrades (p. 2157)	You can now have your RDS for SQL Server DB instances automatically upgraded to the latest minor version. For more information, see Upgrading the Microsoft SQL Server DB engine .	August 13, 2021
Amazon RDS for PostgreSQL now supports PostgreSQL version 14 beta 2 in the database preview environment (p. 2157)	For more about PostgreSQL version 14 beta 1, see PostgreSQL 14 beta 1 release notes . For more about PostgreSQL version 14 beta 2, see PostgreSQL 14 beta 2 release notes . For information on the Database Preview Environment, see Working with the database preview environment .	August 9, 2021
Amazon RDS supports RDS Proxy in a shared VPC (p. 2157)	You can now create an RDS Proxy in a shared VPC. For more information about RDS Proxy, see "Managing Connections with Amazon RDS Proxy" in the Amazon RDS User Guide or the Aurora User Guide .	August 6, 2021
Amazon RDS supports MariaDB 10.2.39 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.2.39. For more information, see MariaDB on Amazon RDS versions .	August 4, 2021
Amazon RDS for Oracle adds the TIMEZONE_FILE_AUTOUPGRADE option (p. 2157)	With this option, you can upgrade the current time zone file to the latest version on your Oracle DB instance. For more information, see Oracle time zone file autoupgrade .	July 30, 2021
Amazon RDS extends support for cross-Region automated backups (p. 2157)	You can now replicate DB snapshots and transaction logs between more AWS Regions. For more information, see Replicating automated backups to another AWS Region .	July 19, 2021

Support for MySQL 5.7.34 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.34. For more information, see MySQL on Amazon RDS versions .	July 8, 2021
Amazon RDS on AWS Outposts supports additional RDS for PostgreSQL versions (p. 2157)	RDS on Outposts now supports RDS for PostgreSQL versions 12.7 and 13.3. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	July 8, 2021
Amazon RDS for PostgreSQL supports oracle_fdw (p. 2157)	You can now use the oracle_fdw extension to provide a foreign data wrapper for access to Oracle databases. For more information, see Accessing external data with the oracle_fdw extension .	July 8, 2021
Amazon RDS supports Oracle Management Agent (OMA) version 13.5 (p. 2157)	You can use Oracle Management Agent (OMA) version 13.5 with Oracle Enterprise Manager (OEM) Cloud Control 13c Release 5 and higher. Amazon RDS for Oracle installs OMA, which then communicates with your Oracle Management Service (OMS) to provide monitoring information. If you run OMS 13.5, you can manage databases by installing OMA 13.5. For more information, see Oracle Management Agent for Enterprise Manager Cloud Control .	July 7, 2021
Amazon RDS for Oracle supports downloading logs from Amazon S3 (p. 2157)	If archived redo logs aren't on your instance but are protected by your backup retention period, you can use <code>rdsadmin.rdsadmin_archive_log_download</code> to download them from Amazon S3. RDS for Oracle saves the logs to the <code>/rdsdbdata/log/arch</code> directory on your DB instance. For more information, see Downloading archived redo logs from Amazon S3 .	July 2, 2021
Amazon RDS supports MariaDB 10.4.18 and 10.5.9 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.4.18 and 10.5.9. For more information, see MariaDB on Amazon RDS versions .	June 30, 2021

Amazon RDS for Oracle supports Database Activity Streams (p. 2157)	You can now monitor an Oracle DB instance using Database Activity Streams. An Oracle database writes audit records to the unified audit trail. When you start a database activity stream on an Oracle DB instance, Amazon Kinesis streams all activities that match the Oracle Database audit policies. For more information, see Monitoring Amazon RDS for Oracle using Database Activity Streams .	June 23, 2021
Amazon RDS for Oracle introduces memory optimized instance classes (p. 2157)	New Oracle DB instance classes are optimized for workloads that require additional memory, storage, and I/O per vCPU. For more information, see RDS for Oracle instance classes .	June 23, 2021
Support for MySQL 8.0.25 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.25. For more information, see MySQL on Amazon RDS versions .	June 18, 2021
Amazon RDS on AWS Outposts supports additional RDS for PostgreSQL versions (p. 2157)	RDS on Outposts now supports RDS for PostgreSQL versions 12.5, 12.6, 13.1, and 13.2. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	May 28, 2021
Amazon RDS supports MariaDB 10.2.37 and 10.3.28 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.2.37 and 10.3.28. For more information, see MariaDB on Amazon RDS versions .	May 27, 2021
Amazon RDS for Oracle supports multitenant container database (CDB) (p. 2157)	A multitenant architecture enables an Oracle database to be a CDB. In Oracle Database 19c, your CDB can include a single PDB. The user experience with a PDB is mostly identical to the user experience with a non-CDB. For more information, see RDS for Oracle architecture .	May 25, 2021
Amazon RDS on AWS Outposts supports Amazon RDS for SQL Server (p. 2157)	RDS on Outposts now supports Amazon RDS for SQL Server. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	May 11, 2021

Amazon RDS extends support for cross-Region automated backups (p. 2157)	You can now configure Amazon RDS database instances running Microsoft SQL Server to replicate DB snapshots and transaction logs to a different AWS Region. For more information, see Replicating automated backups to another AWS Region .	May 7, 2021
Amazon RDS supports cross-Region automated backups for encrypted DB instances (p. 2157)	You can now replicate DB snapshots and transaction logs to a different AWS Region for encrypted Amazon RDS database instances running Oracle or PostgreSQL. For more information, see Replicating automated backups to another AWS Region .	May 3, 2021
Amazon RDS on AWS Outposts supports Amazon CloudWatch monitoring (p. 2157)	RDS on Outposts now supports Amazon CloudWatch monitoring. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	April 21, 2021
RDS for PostgreSQL supports AWS Lambda functions (p. 2157)	You can now invoke AWS Lambda functions for your RDS for PostgreSQL DB instances. For more information, see Invoking an AWS Lambda function from an RDS for PostgreSQL DB instance .	April 13, 2021
RDS for SQL Server supports extended events (p. 2157)	You can use SQL Server extended events to capture debugging and troubleshooting information. For more information, see Using extended events with Amazon RDS for Microsoft SQL Server .	April 8, 2021
Support for MySQL 8.0.23, 5.7.33, and 5.6.51 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.23, 5.7.33, and 5.6.51. For more information, see MySQL on Amazon RDS versions .	March 31, 2021

Automatic rollback on failed Amazon RDS for MySQL upgrade (p. 2157)	If a DB instance upgrade from MySQL version 5.7 to MySQL version 8.0 fails, Amazon RDS rolls back the changes performed for the upgrade automatically. After the rollback, the MySQL DB instance is running MySQL version 5.7. For more information, see Rollback after failure to upgrade from MySQL 5.7 to 8.0 .	March 18, 2021
Amazon RDS supports cross-Region read replicas in opt-in Regions (p. 2157)	You can now replicate DB instances to opt-in Regions. For more information, see Creating a read replica in a different AWS Region .	March 18, 2021
Amazon RDS plans to deprecate Oracle Database 18c (p. 2157)	Oracle Database 18c (18.0.0.0) is on a deprecation path. Oracle Corporation will no longer provide patches for Oracle Database 18c after the end-of-support date. On July 1, 2021, Amazon RDS plans to begin automatically upgrading Oracle Database 18c instances to Oracle Database 19c. Before the automatic upgrades begin, we highly recommend that you manually upgrade your existing Oracle Database 18c instances to Oracle Database 19c. For more information, see Preparing for the automatic upgrade of Oracle Database 18c .	March 11, 2021
Amazon RDS has ended support for Oracle Database 11g (p. 2157)	You can only create DB instances for Oracle Database 12c Release 1 (12.1.0.2) and later. If you have Oracle Database 11g snapshots, upgrade them to a later release. For more information, see Upgrading an Oracle DB snapshot .	March 11, 2021
Amazon RDS supports continuous backups of DB instances in AWS Backup (p. 2157)	You can now create automated backups in AWS Backup and restore DB instances from these backups to a specified time. For more information, see Using AWS Backup to manage automated backups .	March 10, 2021

Amazon RDS supports Oracle Management Agent (OMA) version 13.4 (p. 2157)	You can use Oracle Management Agent (OMA) version 13.4 with Oracle Enterprise Manager (OEM) Cloud Control 13c Release 4 Update 9. Amazon RDS for Oracle installs OMA, which then communicates with your Oracle Management Service (OMS) to provide monitoring information. If you run OMS 13.4, you can manage databases by installing OMA 13.4. For more information, see Oracle Management Agent for Enterprise Manager Cloud Control .	March 10, 2021
RDS Proxy endpoint enhancements (p. 2157)	You can create additional endpoints associated with each RDS proxy. Creating an endpoint in a different VPC enables cross-VPC access for the proxy. Proxies for Aurora MySQL clusters can also have read-only endpoints. These reader endpoints connect to reader DB instances in the clusters and can improve read scalability and availability for query-intensive applications. For more information about RDS Proxy, see "Managing Connections with Amazon RDS Proxy" in the Amazon RDS User Guide or the Aurora user guide .	March 8, 2021
Amazon RDS extends supports for cross-Region automated backups (p. 2157)	You can now configure Amazon RDS database instances running PostgreSQL to replicate DB snapshots and transaction logs to a different AWS Region. For more information, see Replicating automated backups to another AWS Region .	March 8, 2021
Replication filters for Amazon RDS for MariaDB and MySQL supported in the China (Beijing) Region and China (Ningxia) Region (p. 2157)	Replication filtering is now supported in the China (Beijing) Region and China (Ningxia) Region. For more information, see Configuring replication filters with MariaDB and Configuring replication filters with MySQL .	March 5, 2021

Amazon RDS supports cross-Region DB snapshot copy in opt-in Regions (p. 2157)	You can now copy DB snapshots to and from opt-in AWS Regions. For more information, see Copying snapshots across AWS Regions .	March 4, 2021
Amazon RDS for SQL Server supports Always On Availability Groups for Standard Edition (p. 2157)	When you create a DB instance using the Multi-AZ configuration on SQL Server 2019 for the Standard Edition database engine, RDS automatically uses Availability Groups. For more information, see Multi-AZ deployments for Microsoft SQL Server .	February 23, 2021
Amazon RDS for Oracle introduces advisor-related procedures (p. 2157)	The <code>rdsadmin_util</code> package includes the procedures <code>advisor_task_set_parameter</code> , <code>advisor_task_drop</code> , and <code>dbms_stats_init</code> . You can use these procedures to modify, stop, and re-enable advisor tasks such as <code>AUTO_STATS_ADVISOR_TASK</code> . For more information, see Setting parameters for advisor tasks .	February 23, 2021
Amazon RDS provides failover reasons for Multi-AZ DB instances (p. 2157)	You can now see more detailed explanations when a Multi-AZ DB instance fails over to a standby replica. For more information, see Failover process for Amazon RDS .	February 18, 2021
Amazon RDS extends support for exporting snapshots to Amazon S3 (p. 2157)	You can now export DB snapshot data to Amazon S3 in China. For more information, see Exporting DB snapshot data to Amazon S3 .	February 17, 2021
Replication filters for Amazon RDS for MariaDB and MySQL (p. 2157)	You can configure replication filters for MySQL and MariaDB instances. Replication filters specify which databases and tables are replicated in a read replica. You can create lists of databases and tables to include or exclude for each read replica. For more information, see Configuring replication filters with MariaDB and Configuring replication filters with MySQL .	February 12, 2021
RDS for Oracle supports APEX 20.2v1 (p. 2157)	You can use APEX 20.2.v1 with all supported versions of Oracle Database. For more information, see Oracle Application Express .	February 2, 2021

Amazon RDS for SQL Server supports local instance storage for the tempdb database (p. 2157)	You can now launch Amazon RDS for SQL Server on Amazon EC2 db.r5d and db.m5d instance types with the tempdb database configured to use an instance store. By placing tempdb data files and log files locally, you can achieve lower read and write latencies when compared to standard storage based on Amazon EBS. For more information, see Instance store support for the tempdb database on Amazon RDS for SQL Server .	January 27, 2021
Amazon RDS for PostgreSQL supports pg_partman and pg_cron (p. 2157)	Amazon RDS for PostgreSQL now supports the pg_partman and pg_cron extensions. For more information on the pg_partman extension, see Managing PostgreSQL partitions with the pg_partman extension . For more information on the pg_cron extension, see Scheduling maintenance with the PostgreSQL pg_cron extension .	January 12, 2021
Amazon RDS supports publishing the Oracle Management Agent log to Amazon CloudWatch Logs (p. 2157)	The Oracle Management Agent log consists of emctl.log, emdctlj.log, gcagent.log, gcagent_errors.log, emagent.nohup, and secure.log. Amazon RDS publishes each of these logs as a separate CloudWatch log stream. For more information, see Publishing Oracle logs to Amazon CloudWatch Logs .	December 28, 2020
Amazon RDS on AWS Outposts supports additional database versions (p. 2157)	RDS on Outposts now supports additional MySQL and PostgreSQL versions. For more information, see Amazon RDS on AWS Outposts support for Amazon RDS features .	December 23, 2020

Amazon RDS on AWS Outposts supports ColPs (p. 2157)	RDS on Outposts now supports customer-owned IP addresses (ColPs). ColPs provide local or external connectivity to resources in your Outpost subnets through your on-premises network. For more information, see Customer-owned IP addresses for RDS on Outposts .	December 22, 2020
Amazon RDS for Oracle plans upgrade of 11g BYOL instances to 19c (p. 2157)	On January 4, 2021, we plan to begin automatically upgrading all editions of Oracle Database 11g instances on the Bring Your Own License (BYOL) model to Oracle Database 19c. All Oracle Database 11g instances, including reserved instances, will move to the latest available Release Update (RU). For more information, see Preparing for the automatic upgrade of Oracle Database 11g BYOL .	December 11, 2020
Amazon RDS supports replicating automated backups to another AWS Region (p. 2157)	You can now configure your Amazon RDS database instances to replicate snapshots and transaction logs to a destination AWS Region of your choice. For more information, see Replicating automated backups to another AWS Region .	December 4, 2020
Amazon RDS for Oracle and Microsoft SQL Server support a new DB instance class (p. 2157)	You can now use the db.r5b instance class to create Amazon RDS DB instances running Oracle or SQL Server. For more information, see Supported DB engines for DB instance classes .	December 4, 2020
Support for MariaDB 10.2.32 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.2.32. For more information, see MariaDB on Amazon RDS versions .	November 25, 2020
Amazon RDS for SQL Server supports the Microsoft Business Intelligence Suite on SQL Server 2019 (p. 2157)	You can now run SQL Server Analysis Services, SQL Server Integration Services, and SQL Server Reporting Services on DB instances using the latest major version. For more information, see Options for the Microsoft SQL Server database engine .	November 24, 2020

Amazon RDS for PostgreSQL version 13 in the database preview environment (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL version 13. For more information, see PostgreSQL 13 versions .	November 24, 2020
Amazon RDS Performance Insights introduces new dimensions (p. 2157)	You can group database load according to the dimension groups for database (PostgreSQL, MySQL, and MariaDB), application (PostgreSQL), and session type (PostgreSQL). Amazon RDS also supports the dimensions db.name (PostgreSQL, MySQL, and MariaDB), db.application.name (PostgreSQL), and db.session_type.name (PostgreSQL). For more information, see Top load table .	November 24, 2020
Amazon RDS for MariaDB supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.5. For more information, see MariaDB on Amazon RDS versions .	November 23, 2020
Support for MySQL 5.6.49 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.6.49. For more information, see MySQL on Amazon RDS versions .	November 20, 2020
Support for MySQL 5.5.62 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.5.62. For more information, see MySQL on Amazon RDS versions .	November 20, 2020
Performance Insights supports analyzing statistics for running PostgreSQL queries (p. 2157)	You can now analyze statistics for running queries with Performance Insights for PostgreSQL DB instances. For more information, see Statistics for PostgreSQL .	November 18, 2020
Amazon RDS extends support for storage autoscaling (p. 2157)	You can now enable storage autoscaling when creating a read replica, restoring a DB instance to a specified time, or restoring a MySQL DB instance from an Amazon S3 backup. For more information, see Managing capacity automatically with Amazon RDS storage autoscaling .	November 18, 2020

Amazon RDS for SQL Server supports Database Mail (p. 2157)	With Database Mail you can send email messages from your Amazon RDS for SQL Server database instance. After specifying the email recipients, you can add files or query results to the message you send. For more information, see Using Database Mail on Amazon RDS for SQL Server .	November 4, 2020
Support for MySQL 8.0.21 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.21. For more information, see MySQL on Amazon RDS versions .	October 22, 2020
Amazon RDS extends support for exporting snapshots to Amazon S3 (p. 2157)	You can now export DB snapshot data to Amazon S3 in all commercial AWS Regions. For more information, see Exporting DB snapshot data to Amazon S3 .	October 22, 2020
Amazon RDS for PostgreSQL supports read replica upgrades (p. 2157)	With Amazon RDS for PostgreSQL, when you do a major version upgrade of the primary DB instance, read replicas are also automatically upgraded. For more information, see Upgrading the PostgreSQL DB engine .	October 15, 2020
Amazon RDS for MariaDB, MySQL and PostgreSQL support the Graviton2 DB instance classes (p. 2157)	You can now use the Graviton2 DB instance classes db.m6g.x and db.r6g.x to create Amazon RDS DB instances running MariaDB, MySQL or PostgreSQL. For more information, see Supported DB Engines for All Available DB Instance Classes .	October 15, 2020
Amazon RDS for SQL Server supports upgrades to SQL Server 2019 (p. 2157)	You can upgrade your SQL Server DB instances to SQL Server 2019. For more information, see Upgrading the Microsoft SQL Server DB Engine .	October 6, 2020
Amazon RDS for Oracle supports specifying the national character set (p. 2157)	The national character set, also called the NCHAR character set, is used in the NCHAR, NVARCHAR2, and NCLOB data types. When you create a database, you can specify either AL16UTF16 (default) or UTF8 as the NCHAR character set. For more information, see Oracle character sets supported in Amazon RDS .	October 2, 2020

Support for MySQL 5.7.31 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.31. For more information, see MySQL on Amazon RDS versions .	October 1, 2020
Amazon RDS for PostgreSQL supports exporting data to Amazon S3 (p. 2157)	You can query data from a PostgreSQL DB instance and export it directly into files stored in an Amazon S3bucket. For more information, see Exporting data from an RDS for PostgreSQL DB instance to Amazon S3 .	September 24, 2020
Amazon RDS for MySQL 8.0 supports Percona XtraBackup (p. 2157)	You can now use Percona XtraBackup to restore a backup into an Amazon RDS for MySQL 8.0 DB instance. For more information, see Restoring a backup into a MySQL DB instance .	September 17, 2020
Amazon RDS for SQL Server supports native backup and restore on DB instances with read replicas (p. 2157)	You can restore a SQL Server native backup onto a DB instance that has read replicas configured. For more information, see Importing and exporting SQL Server databases .	September 16, 2020
Amazon RDS for SQL Server supports additional time zones (p. 2157)	You can match your DB instance time zone with your chosen time zone. For more information, see Local time zone for Microsoft SQL Server DB instances .	September 11, 2020
Amazon RDS for PostgreSQL version 13 beta 3 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL Version 13 Beta 3 in the Database Preview Environment. For more information, see PostgreSQL 13 versions .	September 9, 2020
Amazon RDS for SQL Server supports trace flag 692 (p. 2157)	You can now use trace flag 692 as a startup parameter using DB parameter groups. Enabling this trace flag disables fast inserts while bulk loading data into heap or clustered indexes. For more information, see Disabling fast inserts during bulk loading .	August 27, 2020
Amazon RDS for SQL Server supports Microsoft SQL Server 2019 (p. 2157)	You can now create RDS DB instances that use SQL Server 2019. For more information, see Microsoft SQL Server versions on Amazon RDS .	August 26, 2020

RDS for Oracle supports mounted replica database (p. 2157)	When creating or modifying an Oracle replica, you can place it in mounted mode. Because the replica database doesn't accept user connections, it can't serve a read-only workload. The mounted replica deletes archived redo log files after it applies them. The primary use for mounted replicas is cross-Region disaster recovery. For more information, see Overview of Oracle replicas .	August 13, 2020
RDS for Oracle plans upgrade of 11g SE1 LI instances (p. 2157)	On November 1, 2020, we plan to begin automatically upgrading Oracle Database 11g SE1 License Included (LI) instances to Oracle Database 19c for Amazon RDS for Oracle. All 11g instances, including reserved instances, will move to the latest available Oracle Release Update (RU). For more information, see Preparing for the automatic upgrade of Oracle Database 11g SE1 .	July 31, 2020
Amazon RDS supports new Graviton2 DB instance classes in preview release for PostgreSQL and MySQL (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL or MySQL that use the db.m6g.x and db.r6g.x DB instance classes. For more information, see Supported DB engines for all available DB instance classes .	July 30, 2020
RDS for Oracle supports APEX 20.1v1 (p. 2157)	You can use APEX 20.1v1 with all supported versions of Oracle Database. For more information, see Oracle application Express .	July 28, 2020
Support for MySQL 8.0.20 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.20. For more information, see MySQL on Amazon RDS versions .	July 23, 2020
Amazon RDS for MariaDB and MySQL support new DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running MariaDB and MySQL that use the db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge, and db.r5.8xlarge DB instance classes. For more information, see Supported DB engines for all available DB instance classes .	July 23, 2020

RDS for SQL Server supports disabling old versions of TLS and ciphers (p. 2157)	You can turn certain security protocols and ciphers on and off. For more information, see Configuring security protocols and ciphers .	July 21, 2020
RDS supports Oracle Spatial on SE2 (p. 2157)	You can use Oracle Spatial in Standard Edition 2 (SE2) for all versions of 12.2, 18c, and 19c. For more information, see Oracle Spatial .	July 9, 2020
Amazon RDS supports AWS PrivateLink (p. 2157)	Amazon RDS now supports creating Amazon VPC endpoints for Amazon RDS API calls to keep traffic between applications and Amazon RDS in the AWS network. For more information, see Amazon RDS and interface VPC endpoints (AWS PrivateLink) .	July 9, 2020
Amazon RDS for PostgreSQL versions 9.4.x has reached its end of support. (p. 2157)	Amazon RDS for PostgreSQL no longer supports versions 9.4.x. For supported versions, see Supported PostgreSQL database versions .	July 8, 2020
Support for MariaDB 10.3.23 and 10.4.13 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.3.23 and 10.4.13. For more information, see MariaDB on Amazon RDS versions .	July 6, 2020
Amazon RDS on AWS Outposts (p. 2157)	You can create Amazon RDS DB instances on AWS Outposts. For more information, see Working with Amazon RDS on AWS Outposts .	July 6, 2020
Amazon RDS for Oracle creates inventory files automatically (p. 2157)	To open service requests for BYOL customers, Oracle Support requests inventory files generated by Opatch. Amazon RDS for Oracle automatically creates inventory files every hour in the BDUMP directory. For more information, see Accessing Opatch files .	July 6, 2020
Support for MySQL 5.7.30 and 5.6.48 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.30 and 5.6.48. For more information, see MySQL on Amazon RDS versions .	June 25, 2020

Amazon RDS for Oracle supports ADRCI (p. 2157)	The Automatic Diagnostic Repository Command Interpreter (ADRCI) utility is an Oracle command-line tool that you use to manage diagnostic data. By using the functions in the Amazon RDS package <code>rdsadmin_adrci_util</code> , you can list and package problems and incidents, and also show trace files. For more information, see Common DBA diagnostic tasks for Oracle DB instances .	June 17, 2020
Support for MySQL 8.0.19 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.19. For more information, see MySQL on Amazon RDS versions .	June 2, 2020
MySQL 8.0 supports lower case table names (p. 2157)	You can now set the <code>lower_case_table_names</code> parameter to 1 for Amazon RDS DB instances running MySQL version 8.0.19 and higher 8.0 versions. For more information, see MySQL parameter exceptions for Amazon RDS DB instances .	June 2, 2020
Amazon RDS for Microsoft SQL Server supports SQL Server Integration Services (SSIS) (p. 2157)	SSIS is a platform for data integration and workflow applications. You can enable SSIS on existing or new DB instances. It's installed on the same DB instance as your database engine. For more information, see Support for SQL Server Integration Services in SQL Server .	May 19, 2020
Amazon RDS for Microsoft SQL Server supports SQL Server Reporting Services (SSRS) (p. 2157)	SSRS is a server-based application used for report generation and distribution. You can enable SSRS on existing or new DB instances. It's installed on the same DB instance as your database engine. For more information, see Support for SQL Server Reporting Services in SQL Server .	May 15, 2020

Amazon RDS for Microsoft SQL Server supports S3 integration on Multi-AZ instances (p. 2157)	You can now use Amazon S3 with SQL Server features such as bulk insert on Multi-AZ DB instances. For more information, see Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 .	May 15, 2020
Amazon RDS for Oracle supports purging the recycle bin (p. 2157)	The <code>rdsadmin.rdsadmin_util.purge_dba_recyclebin</code> procedure purges the recycle bin. For more information, see Purging the recycle bin .	May 13, 2020
Amazon RDS for Oracle improves manageability of Automatic Workload Repository (AWR) (p. 2157)	The <code>rdsadmin.rdsadmin_diagnostic_util</code> procedures generate AWR reports and extract AWR data into dump files. For more information, see Generating performance reports with Automatic Workload Repository (AWR) .	May 13, 2020
Amazon RDS for Microsoft SQL Server supports Microsoft Distributed Transaction Coordinator (MSDTC) (p. 2157)	Amazon RDS for SQL Server supports distributed transactions between hosts. For more information, see Support for Microsoft Distributed Transaction Coordinator in SQL Server .	May 4, 2020
Amazon RDS for Microsoft SQL Server supports new versions (p. 2157)	You can now create Amazon RDS DB instances running SQL Server versions 2017 CU19 14.00.3281.6, 2016 SP2 CU11 13.00.5598.27, 2014 SP3 CU4 12.00.6329.1, and 2012 SP4 GDR 11.0.7493.4 for all editions. For more information, see Microsoft SQL Server versions on Amazon RDS .	April 28, 2020
Amazon RDS available in the Europe (Milan) Region (p. 2157)	Amazon RDS is now available in the Europe (Milan) Region. For more information, see Regions and Availability Zones .	April 28, 2020
Amazon RDS support for Local Zones (p. 2157)	You can now launch DB instances into a Local Zone subnet. For more information, see Regions, Availability Zones, and Local Zones .	April 23, 2020
Amazon RDS available in the Africa (Cape Town) Region (p. 2157)	Amazon RDS is now available in the Africa (Cape Town) Region. For more information, see Regions and Availability Zones .	April 22, 2020

Amazon RDS for Microsoft SQL Server supports SQL Server Analysis Services (SSAS) (p. 2157)	SSAS is an online analytical processing (OLAP) and data mining tool that is installed within SQL Server. You can enable SSAS on existing or new DB instances. It's installed on the same DB instance as your database engine. For more information, see Support for SQL Server Analysis Services in SQL Server .	April 17, 2020
Amazon RDS proxy for PostgreSQL (p. 2157)	Amazon RDS Proxy is now available for PostgreSQL. You can use RDS Proxy to reduce the overhead of connection management on your DB instance and also the chance of "too many connections" errors. The RDS Proxy is currently in public preview for PostgreSQL. For more information, see Managing connections with Amazon RDS proxy (preview) .	April 8, 2020
Amazon RDS for Oracle supports Oracle APEX version 19.2.v1 (p. 2157)	Amazon RDS for Oracle now supports Oracle Application Express (APEX) version 19.2.v1. For more information, see Oracle application Express .	April 8, 2020
Amazon RDS for MariaDB supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.4. For more information, see MariaDB on Amazon RDS versions .	April 6, 2020
Amazon RDS Performance Insights is available for Amazon RDS for MariaDB 10.4 (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for MariaDB version 10.4. For more information, see Using Amazon RDS performance insights .	April 6, 2020
Amazon RDS for PostgreSQL versions 9.3.x has reached its end of support (p. 2157)	Amazon RDS for PostgreSQL no longer supports versions 9.3.x. For supported versions, see Supported PostgreSQL database versions .	April 3, 2020
Amazon RDS for Microsoft SQL Server supports read replicas (p. 2157)	You can now create read replicas for SQL Server DB instances. For more information, see Working with read replicas .	April 3, 2020

Amazon RDS for Microsoft SQL Server supports multifile backups (p. 2157)	You can now back up databases to multiple files using SQL Server native backup and restore. For more information, see Backing up a database .	April 2, 2020
Amazon RDS for Oracle integration with AWS License Manager (p. 2157)	Amazon RDS for Oracle is now integrated with AWS License Manager. If you use the Bring Your Own License model, AWS License Manager integration makes it easier to monitor your Oracle license usage within your organization. For more information, see Integrating with AWS License Manager .	March 23, 2020
Support for 64 TiB on db.r5 instances in Amazon RDS for MariaDB and MySQL (p. 2157)	You can now create Amazon RDS DB instances for MariaDB and MySQL that use the db.r5 DB instance class with up to 64 TiB of storage. For more information, see Factors that affect storage performance .	March 18, 2020
Support for MySQL 8.0.17 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.17. For more information, see MySQL on Amazon RDS versions .	March 10, 2020
Amazon RDS Performance Insights is available for Amazon RDS for MySQL 8.0 (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for MySQL version 8.0.17 and higher 8.0 versions. For more information, see Using Amazon RDS performance insights .	March 10, 2020
Support for MySQL 5.6.46 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.6.46. For more information, see MySQL on Amazon RDS versions .	February 28, 2020
Amazon RDS Performance Insights is available for Amazon RDS for MariaDB 10.3 (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for MariaDB version 10.3.13 and higher 10.3 versions. For more information, see Using Amazon RDS performance insights .	February 26, 2020
Support for MySQL 5.7.28 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.28. For more information, see MySQL on Amazon RDS versions .	February 20, 2020

Support for MariaDB 10.3.20 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.3.20. For more information, see MariaDB on Amazon RDS versions .	February 20, 2020
Amazon RDS for Microsoft SQL Server supports a new DB instance class (p. 2157)	You can now create Amazon RDS DB instances running SQL Server that use the db.z1d DB instance class. For more information, see DB instance class support for Microsoft SQL Server .	February 19, 2020
Support for cross-account, cross-VPC Active Directory domains in Amazon RDS for SQL Server (p. 2157)	Amazon RDS for Microsoft SQL Server now supports associating DB instances with Active Directory domains owned by different accounts and VPCs. For more information, see Using Windows authentication with a Microsoft SQL Server DB instance .	February 13, 2020
Oracle OLAP option (p. 2157)	Amazon RDS for Oracle now supports the On-line Analytical Processing (OLAP) option for Oracle DB instances. You can use Oracle OLAP to analyze large amounts of data by creating dimensional objects and cubes in accordance with the OLAP standard. For more information, see Oracle OLAP .	February 13, 2020
FIPS 140-2 support for Oracle (p. 2157)	Amazon RDS for Oracle supports the Federal Information Processing Standard Publication 140-2 (FIPS 140-2) for SSL/TLS connections. For more information, see FIPS support .	February 11, 2020
Amazon RDS for PostgreSQL supports new DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL that use the db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge, and db.r5.8xlarge DB instance classes. For more information, see Supported DB engines for all available DB instance classes .	February 11, 2020
Performance Insights supports analyzing statistics of running MariaDB and MySQL queries (p. 2157)	You can now analyze statistics of running queries with Performance Insights for MariaDB and MySQL DB instances. For more information, see Analyzing statistics of running queries .	February 4, 2020

Support for exporting DB snapshot data to Amazon S3 for MariaDB, MySQL, and PostgreSQL (p. 2157)	Amazon RDS supports exporting DB snapshot data to Amazon S3 for MariaDB, MySQL, and PostgreSQL. For more information, see Exporting DB snapshot data to Amazon S3 .	January 23, 2020
Amazon RDS for MySQL supports Kerberos authentication (p. 2157)	You can now use Kerberos authentication to authenticate users when they connect to your Amazon RDS for MySQL DB instances. For more information, see Using Kerberos authentication for MySQL .	January 21, 2020
Amazon RDS Performance Insights supports viewing more SQL text for Amazon RDS for Microsoft SQL Server (p. 2157)	Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for Amazon RDS for Microsoft SQL Server DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard .	December 17, 2019
Amazon RDS proxy (p. 2157)	You can reduce the overhead of connection management on your cluster, and reduce the chance of "too many connections" errors, by using the Amazon RDS Proxy. You associate each proxy with an RDS DB instance or Aurora DB cluster. Then you use the proxy endpoint in the connection string for your application. The Amazon RDS Proxy is currently in a public preview state. It supports the RDS for MySQL database engine. For more information, see Managing connections with Amazon RDS proxy (preview) .	December 3, 2019
Amazon RDS on AWS Outposts (preview) (p. 2157)	With Amazon RDS on AWS Outposts, you can create AWS-managed relational databases in your on-premises data centers. RDS on Outposts enables you to run RDS databases on AWS Outposts. For more information, see Amazon RDS on AWS Outposts (preview) .	December 3, 2019

Amazon RDS for Oracle supports cross-region read replicas (p. 2157)	Amazon RDS for Oracle now supports cross-region read replicas with Active Data Guard. For more information, see Working with read replicas and Working with Oracle read replicas .	November 26, 2019
Performance Insights supports analyzing statistics of running Oracle queries (p. 2157)	You can now analyze statistics of running queries with Performance Insights for Oracle DB instances. For more information, see Analyzing statistics of running queries .	November 25, 2019
Amazon RDS for Microsoft SQL Server supports publishing logs to CloudWatch Logs (p. 2157)	You can configure your Amazon RDS for SQL Server DB instance to publish log events directly to Amazon CloudWatch Logs. For more information, see Publishing SQL Server logs to Amazon CloudWatch Logs .	November 25, 2019
Amazon RDS for Microsoft SQL Server supports new DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running SQL Server that use the db.x1e and db.x1 DB instance classes. For more information, see DB instance class support for Microsoft SQL Server .	November 25, 2019
Amazon RDS for Microsoft SQL Server supports differential and log restores (p. 2157)	You can restore differential backups and logs using SQL Server native backup and restore. For more information, see Using native backup and restore .	November 25, 2019
Multi-AZ supported on Amazon RDS for Microsoft SQL Server in new regions (p. 2157)	Multi-AZ on SQL Server is now available in China, Middle East (Bahrain), and Europe (Stockholm). For more information, see Multi-AZ deployments for Microsoft SQL Server .	November 22, 2019
Amazon RDS for Microsoft SQL Server now supports bulk insert and S3 integration (p. 2157)	You can transfer files between a SQL Server DB instance and an Amazon S3 bucket. Then you can use Amazon S3 with SQL Server features such as bulk insert. For more information, see Integrating an Amazon RDS for SQL Server DB instance with Amazon S3 .	November 21, 2019

Performance Insights counters for Amazon RDS for Microsoft SQL Server (p. 2157)	You can now add performance counters to your Performance Insights charts for Microsoft SQL Server DB instances. For more information, see Performance Insights counters for Amazon RDS for Microsoft SQL Server .	November 12, 2019
Amazon RDS for Microsoft SQL Server supports new DB instance class sizes (p. 2157)	You can now create Amazon RDS DB instances running SQL Server that use the 8xlarge and 16xlarge instance sizes for the db.m5 and db.r5 DB instance classes. Instance sizes ranging from small to 2xlarge are now available for the db.t3 instance class. For more information, see DB instance class support for Microsoft SQL Server .	November 11, 2019
Support for PostgreSQL snapshot upgrades (p. 2157)	If you have existing manual DB snapshots of your Amazon RDS PostgreSQL DB instances, you can now upgrade them to a later version of the PostgreSQL database engine. For more information, see Upgrading a PostgreSQL DB snapshot .	November 7, 2019
Amazon RDS for Oracle supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running Oracle Database 19c (19.0). For more information, see Oracle Database 19c with Amazon RDS .	November 7, 2019
Amazon RDS for PostgreSQL version 12.0 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL Version 12.0 in the Database Preview Environment. For more information, see PostgreSQL version 12.0 in the database preview environment .	November 1, 2019
Amazon RDS for PostgreSQL supports Kerberos authentication (p. 2157)	You can now use Kerberos authentication to authenticate users when they connect to your Amazon RDS DB instance running PostgreSQL. For more information, see Using Kerberos authentication with Amazon RDS for PostgreSQL .	October 28, 2019

OEM Management Agent database tasks for Oracle DB instances (p. 2157)	Amazon RDS for Oracle DB instances now support procedures to invoke certain EMCTL commands on the Management Agent. For more information, see OEM agent database tasks .	October 24, 2019
Amazon RDS for PostgreSQL supports PostgreSQL transportable databases (p. 2157)	PostgreSQL Transportable Databases provide an extremely fast method of migrating an RDS PostgreSQL database between two DB instances. For more information, see Transporting PostgreSQL databases between DB instances .	October 8, 2019
Amazon RDS for Oracle supports Kerberos authentication (p. 2157)	You can now use Kerberos authentication to authenticate users when they connect to your Amazon RDS DB instance running Oracle. For more information, see Using Kerberos authentication with Amazon RDS for Oracle .	September 30, 2019
Amazon RDS for PostgreSQL version 12 beta 3 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL Version 12 Beta 3 in the Database Preview Environment. For more information, see PostgreSQL version 12 beta 3 on Amazon RDS in the database preview environment .	August 28, 2019
Support for MySQL 8.0.16 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.16. For more information, see MySQL on Amazon RDS versions .	August 19, 2019
Amazon RDS for Oracle supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running Oracle Database 18c (18.0). For more information, see Oracle Database 18c with Amazon RDS .	August 15, 2019
Management Agent for OEM 13c release 3 (p. 2157)	Amazon RDS for Oracle DB instances now support the Management Agent for Oracle Enterprise Manager (OEM) Cloud Control 13c Release 3. For more information, see Oracle Management Agent for Enterprise Manager cloud control .	August 7, 2019

Amazon RDS for PostgreSQL version 12 beta 2 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL Version 12 Beta 2 in the Database Preview Environment. For more information, see PostgreSQL version 12 beta 2 on Amazon RDS in the database preview environment .	August 6, 2019
Amazon RDS supports server collations for SQL Server (p. 2157)	Amazon RDS for SQL Server supports a selection of collations for new DB instances. For more information, see Collations and character sets for Microsoft SQL Server .	July 29, 2019
Amazon RDS for Oracle supports Oracle APEX version 19.1.v1 (p. 2157)	Amazon RDS for Oracle now supports Oracle Application Express (APEX) version 19.1.v1. For more information, see Oracle application Express .	June 28, 2019
Amazon RDS for PostgreSQL version 13 beta 1 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL Version 13 Beta 1 in the Database Preview Environment. For more information, see PostgreSQL 13 versions .	June 22, 2019
Amazon RDS storage autoscaling (p. 2157)	Storage autoscaling for Amazon RDS DB instances enables Amazon RDS to automatically expand the storage associated with a DB instance to reduce the chance of out-of-space conditions. For information about storage autoscaling, see Working with storage for Amazon RDS DB instances .	June 20, 2019
Amazon RDS for Oracle supports db.z1d DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running Oracle that use the db.z1d DB instance classes. For more information, see DB instance class .	June 13, 2019
Amazon RDS Performance Insights supports viewing more SQL text for Amazon RDS for Oracle (p. 2157)	Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for Amazon RDS for Oracle DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard .	June 10, 2019

Amazon RDS adds support native restores of SQL Server databases up to 16 TB (p. 2157)	You can now do native restores of up to 16 TB from SQL Server to Amazon RDS. For more information, see Amazon RDS for SQL Server: Limitations and recommendations .	June 4, 2019
Amazon RDS adds support for Microsoft SQL Server audit (p. 2157)	Using Amazon RDS for Microsoft SQL Server, you can audit server and database level events using SQL Server Audit, and view the results on your DB instance or send the audit log files directly to Amazon S3. For more information, see SQL Server Audit .	May 23, 2019
Improvements to Amazon RDS recommendations (p. 2157)	Amazon RDS has improved its automated recommendations for database resources. For example, Amazon RDS now provides recommendations for database parameters. For more information, see Using Amazon RDS recommendations .	May 22, 2019
Support for more databases per DB instance for Amazon RDS for SQL Server (p. 2157)	You can create up to 30 databases on each of your DB instances running Microsoft SQL Server. For more information, see Limits for Microsoft SQL Server DB instances .	May 21, 2019
Support for 64 TiB and 80k IOPS of storage for Amazon RDS for MariaDB, MySQL and PostgreSQL (p. 2157)	You can now create Amazon RDS DB instances for MariaDB, MySQL and PostgreSQL with up to 64 TiB of storage and up to 80,000 provisioned IOPS. For more information, see DB instance storage .	May 20, 2019
Amazon RDS for MySQL supports upgrade prechecks (p. 2157)	When you upgrade a DB instance from MySQL 5.7 to MySQL 8.0, Amazon RDS performs prechecks for incompatibilities. For more information, see Prechecks for upgrades from MySQL 5.7 to 8.0 .	May 17, 2019
Support for the MySQL password validation plugin (p. 2157)	You can now use the MySQL validate_password plugin for improved security of Amazon RDS for MySQL DB instances. For more information, see Using the Password Validation Plugin .	May 16, 2019

Performance Insights counters for Amazon RDS for Oracle (p. 2157)	You can now add performance counters to your Performance Insights charts for Oracle DB instances. For more information, see Performance Insights counters for Amazon RDS for Oracle .	May 8, 2019
Support for per-second billing (p. 2157)	Amazon RDS is now billed in 1-second increments in all AWS Regions except AWS GovCloud (US) for on-demand instances. For more information, see DB instance billing for Amazon RDS .	April 25, 2019
Support for importing data from Amazon S3 for Amazon RDS for PostgreSQL (p. 2157)	You can now import data from Amazon S3 file into a table in an RDS PostgreSQL DB instance. For more information, see Importing Amazon S3 data into an RDS PostgreSQL DB instance .	April 24, 2019
Support for restoring 5.7 backups from Amazon S3 (p. 2157)	You can now create a backup of your MySQL version 5.7 database, store it on Amazon S3, and then restore the backup file onto a new Amazon RDS DB instance running MySQL. For more information, see Restoring a backup into a MySQL DB instance .	April 17, 2019
Support for multiple major version upgrades for Amazon RDS for PostgreSQL (p. 2157)	With Amazon RDS for PostgreSQL, you can now choose from multiple major versions when you upgrade the DB engine. This feature enables you to skip ahead to a newer major version when you upgrade select PostgreSQL engine versions. For more information, see Upgrading the PostgreSQL DB engine .	April 16, 2019
Support for 64 TiB of storage for Amazon RDS for Oracle (p. 2157)	You can now create Amazon RDS DB instances for Oracle with up to 64 TiB of storage and up to 80,000 provisioned IOPS. For more information, see DB instance storage .	April 4, 2019
Support for MySQL 8.0.15 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0.15. For more information, see MySQL on Amazon RDS versions .	April 3, 2019

Support for MariaDB 10.3.13 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.3.13. For more information, see MariaDB on Amazon RDS versions .	April 3, 2019
Microsoft SQL Server 2008 R2 has reached its end of support on Amazon RDS (p. 2157)	Microsoft SQL Server 2008 R2 has reached its end of support, coinciding with the Microsoft plan to end extended support for this version on July 9, 2019. Any existing Microsoft SQL Server 2008 R2 snapshots are to be automatically upgraded to the latest minor version of Microsoft SQL Server 2012 starting on June 1, 2019. For more information, see Microsoft SQL Server 2008 R2 support on Amazon RDS .	April 2, 2019
Always On availability groups supported in Microsoft SQL Server 2017 (p. 2157)	You can now use Always On Availability Groups in SQL Server 2017 Enterprise Edition 14.00.3049.1 or later. For more information, see Multi-AZ deployments for Microsoft SQL Server .	March 29, 2019
View volume metrics (p. 2157)	You can now view metrics for the Amazon Elastic Block Store (Amazon EBS) volumes, which are the physical devices used for database and log storage. For more information, see Viewing Enhanced Monitoring .	March 20, 2019
Support for MySQL 5.7.25 (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 5.7.25. For more information, see MySQL on Amazon RDS versions .	March 19, 2019
Amazon RDS for Oracle supports RMAN DBA tasks (p. 2157)	Amazon RDS for Oracle now supports Oracle Recovery Manager (RMAN) DBA tasks, including RMAN backups. For more information, see Common DBA Recovery Manager (RMAN) tasks for Oracle DB instances .	March 14, 2019
Amazon RDS for PostgreSQL supports version 11.1 (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL version 11.1. For more information, see PostgreSQL version 11.1 on Amazon RDS .	March 12, 2019

Multiple-file restore is available in Amazon RDS for SQL Server (p. 2157)	You can now restore from multiple files with Amazon RDS for SQL Server. For more information, see Restoring a database .	March 11, 2019
MariaDB 10.2.21 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.2.21. For more information, see MariaDB on Amazon RDS versions .	March 11, 2019
Amazon RDS for Oracle supports read replicas (p. 2157)	Amazon RDS for Oracle now supports read replicas with Active Data Guard. For more information, see Working with read replicas and Working with Oracle read replicas .	March 11, 2019
Amazon RDS Performance Insights is available for Amazon RDS for MariaDB (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for MariaDB. For more information, see Using Amazon RDS Performance Insights .	March 11, 2019
MySQL 8.0.13 and 5.7.24 (p. 2157)	You can now create Amazon RDS DB instances running MySQL versions 8.0.13 and 5.7.24. For more information, see MySQL on Amazon RDS versions .	March 8, 2019
Amazon RDS Performance Insights is available for Amazon RDS for SQL Server (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for SQL Server. For more information, see Using Amazon RDS Performance Insights .	March 4, 2019
Amazon RDS for Oracle supports Amazon S3 integration (p. 2157)	You can now transfer files between an Amazon RDS for Oracle DB instance and an Amazon S3 bucket. For more information, see Integrating Amazon RDS for Oracle and Amazon S3 .	February 26, 2019
Amazon RDS for MySQL and Amazon RDS for MariaDB support db.t3 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running MySQL or MariaDB that use the db.t3 DB instance classes. For more information, see DB instance class .	February 20, 2019

Amazon RDS for MySQL and Amazon RDS for MariaDB support db.r5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running MySQL or MariaDB that use the db.r5 DB instance classes. For more information, see DB instance class .	February 20, 2019
Performance Insights counters for RDS for MySQL and PostgreSQL (p. 2157)	You can now add performance counters to your Performance Insights charts for MySQL and PostgreSQL DB instances. For more information, see Performance Insights dashboard components .	February 19, 2019
Amazon RDS for PostgreSQL now supports adaptive autovacuum parameter tuning (p. 2157)	Adaptive autovacuum parameter tuning with Amazon RDS for PostgreSQL helps prevent transaction ID wraparound by adjusting autovacuum parameter values automatically. For more information, see Reducing the likelihood of transaction ID wraparound .	February 12, 2019
Amazon RDS for Oracle supports Oracle APEX versions 18.1.v1 and 18.2.v1 (p. 2157)	Amazon RDS for Oracle now supports Oracle Application Express (APEX) versions 18.1.v1 and 18.2.v1. For more information, see Oracle application Express .	February 11, 2019
Amazon RDS Performance Insights supports viewing more SQL text for RDS for MySQL (p. 2157)	Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for MySQL DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard .	February 6, 2019
Amazon RDS for PostgreSQL supports db.t3 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL that use the db.t3 DB instance classes. For more information, see DB instance class .	January 25, 2019
Amazon RDS for Oracle supports db.t3 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running Oracle that use the db.t3 DB instance classes. For more information, see DB instance class .	January 25, 2019

Amazon RDS Performance Insights supports viewing more SQL text for Amazon RDS PostgreSQL (p. 2157)	Amazon RDS Performance Insights now supports viewing more SQL text in the Performance Insights dashboard for Amazon RDS PostgreSQL DB instances. For more information, see Viewing more SQL text in the Performance Insights dashboard .	January 24, 2019
Amazon RDS for Oracle supports a new version of SQLT (p. 2157)	Amazon RDS for Oracle now supports SQLT version 12.2.180725. For more information, see Oracle SQLT .	January 22, 2019
Amazon RDS for PostgreSQL supports db.r5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL that use the db.r5 DB instance classes. For more information, see DB instance class .	December 19, 2018
Amazon RDS for PostgreSQL now supports restricted password management (p. 2157)	Amazon RDS for PostgreSQL enables you to restrict who can manage user passwords and password expiration changes by using the parameter <code>rds.restrict_password_commands</code> and the role <code>rds_password</code> . For more information, see Restricting password management .	December 19, 2018
Amazon RDS for PostgreSQL supports uploading database logs to Amazon CloudWatch Logs (p. 2157)	Amazon RDS for PostgreSQL supports uploading database logs to CloudWatch Logs. For more information, see Publishing PostgreSQL logs to CloudWatch Logs .	December 10, 2018
Amazon RDS for Oracle supports db.r5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running Oracle that use the db.r5 DB instance classes. For more information, see DB instance class .	November 20, 2018
Retain backups when deleting a DB instance (p. 2157)	Amazon RDS supports retaining automated backups when you delete a DB instance. For more information, see Working with backups .	November 15, 2018
Amazon RDS for PostgreSQL supports db.m5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running PostgreSQL that use the db.m5 DB instance classes. For more information, see DB instance class .	November 15, 2018

Amazon RDS for Oracle supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running Oracle version 12.2. For more information, see Oracle Database 12c Release 2 (12.2.0.1) with Amazon RDS .	November 13, 2018
Amazon RDS for SQL Server supports Always On (p. 2157)	Amazon RDS for SQL Server supports Always On Availability Groups. For more information, see Multi-AZ deployments for Microsoft SQL Server .	November 8, 2018
Amazon RDS for PostgreSQL supports outbound network access using custom DNS servers (p. 2157)	Amazon RDS for PostgreSQL supports outbound network access using custom DNS servers. For more information, see Using a custom DNS server for outbound network access .	November 8, 2018
Amazon RDS for MariaDB, MySQL, and PostgreSQL supports 32 TiB of storage (p. 2157)	You can now create Amazon RDS DB instances with up to 32 TiB of storage for MySQL, MariaDB, and PostgreSQL. For more information, see DB instance storage .	November 7, 2018
Amazon RDS for Oracle supports extended data types (p. 2157)	You can now enable extended data types on Amazon RDS DB instances running Oracle. With extended data types, the maximum size is 32,767 bytes for the VARCHAR2, NVARCHAR2, and RAW data types. For more information, see Using extended data types .	November 6, 2018
Amazon RDS for Oracle supports db.m5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running Oracle that use the db.m5 DB instance classes. For more information, see DB instance class .	November 2, 2018
Amazon RDS for Oracle migration from SE, SE1, or SE2 to EE (p. 2157)	You can now migrate from any Oracle Database Standard Edition (SE, SE1, or SE2) to Oracle Database Enterprise Edition (EE). For more information, see Migrating between Oracle editions .	October 31, 2018

Amazon RDS can now stop Multi-AZ instances (p. 2157)	Amazon RDS can now stop a DB instance that is part of a Multi-AZ deployment. Formerly, the stop instance feature had a limitation for multi-AZ instances. For more information, see Stopping an Amazon RDS DB instance temporarily .	October 29, 2018
Amazon RDS Performance Insights is available for Amazon RDS for Oracle (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for Oracle. For more information, see Using Amazon RDS Performance Insights .	October 29, 2018
Amazon RDS for PostgreSQL supports PostgreSQL version 11 in the database preview environment (p. 2157)	Amazon RDS for PostgreSQL now supports PostgreSQL version 11 in the Database Preview Environment. For more information, see PostgreSQL version 11 on Amazon RDS in the database preview environment .	October 25, 2018
MySQL supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running MySQL version 8.0. For more information, see MySQL on Amazon RDS versions .	October 23, 2018
MariaDB supports a new major version (p. 2157)	You can now create Amazon RDS DB instances running MariaDB version 10.3. For more information, see MariaDB on Amazon RDS versions .	October 23, 2018
Amazon RDS for Oracle supports Oracle JVM (p. 2157)	Amazon RDS for Oracle now supports the Oracle Java Virtual Machine (JVM) option. For more information, see Oracle Java virtual machine .	October 16, 2018
Custom parameter group for restore and point in time recovery (p. 2157)	You can now specify a custom parameter group when you restore a snapshot or perform a point in time recovery operation. For more information, see Restoring from a DB snapshot and Restoring a DB instance to a specified time .	October 15, 2018
Amazon RDS for Oracle supports 32 TiB storage (p. 2157)	You can now create Oracle RDS DB instances with up to 32 TiB of storage. For more information, see DB instance storage .	October 15, 2018

Amazon RDS for MySQL supports GTIDs (p. 2157)	Amazon RDS for MySQL now supports global transaction identifiers (GTIDs), which are unique across all DB instances and in a replication configuration. For more information, see Using GTID-based replication for RDS for MySQL .	October 10, 2018
MySQL 5.7.23, 5.6.41, and 5.5.61 (p. 2157)	You can now create Amazon RDS DB instances running MySQL versions 5.7.23, 5.6.41, and 5.5.61. For more information, see MySQL on Amazon RDS versions .	October 8, 2018
Amazon RDS for Oracle supports a new version of SQLT (p. 2157)	Amazon RDS for Oracle now supports SQLT version 12.2.180331. For more information, see Oracle SQLT .	October 4, 2018
Amazon RDS for PostgreSQL now supports IAM authentication (p. 2157)	Amazon RDS for PostgreSQL now supports IAM authentication. For more information see IAM database authentication for MySQL and PostgreSQL .	September 27, 2018
You can enable deletion protection for your Amazon RDS DB instances (p. 2157)	When you enable deletion protection for a DB instance, the database cannot be deleted by any user. For more information, see Deleting a DB instance .	September 26, 2018
Amazon RDS for MySQL and Amazon RDS for MariaDB support db.m5 DB instance classes (p. 2157)	You can now create Amazon RDS DB instances running MySQL or MariaDB that use the db.m5 DB instance classes. For more information, see DB instance class .	September 18, 2018
Amazon RDS now supports upgrades to SQL Server 2017 (p. 2157)	You can upgrade your existing DB instance to SQL Server 2017 from any version except SQL Server 2008. To upgrade from SQL Server 2008, first upgrade to one of the other versions first. For information, see Upgrading the Microsoft SQL Server DB engine .	September 11, 2018

Amazon RDS for PostgreSQL now supports PostgreSQL version 11 beta 3 in the database preview environment (p. 2157)	In this release, the Write-Ahead Log (WAL) segment size (<code>wal_segment_size</code>) is now set to 64MB. For more about PostgreSQL version 11 Beta 3, see PostgreSQL 11 beta 3 released . For information on the Database Preview Environment, see Working with the database preview environment .	September 7, 2018
Amazon Aurora User Guide (p. 2157)	The Amazon Aurora User Guide describes all Amazon Aurora concepts and provides instructions on using the various features with both the console and the command line interface. The Amazon RDS User Guide now covers non-Aurora database engines.	August 31, 2018
Amazon RDS Performance Insights is available for RDS for MySQL (p. 2157)	Amazon RDS Performance Insights is now available for RDS for MySQL. For more information, see Using Amazon RDS Performance Insights .	August 28, 2018
Aurora PostgreSQL-Compatible Edition now supports Aurora Auto Scaling (p. 2157)	Auto Scaling of Aurora replicas is now available for Aurora PostgreSQL-Compatible Edition. For more information, see Using Amazon Aurora auto scaling with Aurora replicas .	August 16, 2018
Aurora Serverless for Aurora MySQL (p. 2157)	Aurora Serverless is an on-demand, autoscaling configuration for Amazon Aurora. For more information, see Using Amazon Aurora Serverless .	August 9, 2018
MySQL 5.7.22 and 5.6.40 (p. 2157)	You can now create Amazon RDS DB instances running MySQL versions 5.7.22 and 5.6.40. For more information, see MySQL on Amazon RDS versions .	August 6, 2018
Aurora is now available in the China (Ningxia) region (p. 2157)	Aurora MySQL and Aurora PostgreSQL are now available in the China (Ningxia) region. For more information, see Availability for Amazon Aurora MySQL and Availability for Amazon Aurora PostgreSQL .	August 6, 2018

Amazon RDS for MySQL now supports delayed replication (p. 2157)	Amazon RDS for MySQL now supports delayed replication as a strategy for disaster recovery. For more information, see Configuring delayed replication with MySQL .	August 6, 2018
Amazon RDS Performance Insights is available for Aurora MySQL (p. 2157)	Amazon RDS Performance Insights is now available for Aurora MySQL. For more information, see Using Amazon RDS Performance Insights .	August 6, 2018
Amazon RDS Performance Insights integration with Amazon CloudWatch (p. 2157)	Amazon RDS Performance Insights automatically publishes metrics to Amazon CloudWatch. For more information, see Performance Insights metrics published to CloudWatch .	August 6, 2018
Amazon RDS recommendations (p. 2157)	Amazon RDS now provides automated recommendations for database resources. For more information, see Using Amazon RDS recommendations .	July 25, 2018
Incremental snapshot copies across AWS Regions (p. 2157)	Amazon RDS supports incremental snapshot copies across AWS Regions for both unencrypted and encrypted instances. For more information, see Copying snapshots across AWS Regions .	July 24, 2018
Amazon RDS Performance Insights is available for Amazon RDS for PostgreSQL (p. 2157)	Amazon RDS Performance Insights is now available for Amazon RDS for PostgreSQL. For more information, see Using Amazon RDS Performance Insights .	July 18, 2018
Amazon RDS for Oracle supports Oracle APEX version 5.1.4.v1 (p. 2157)	Amazon RDS for Oracle now supports Oracle Application Express (APEX) version 5.1.4.v1. For more information, see Oracle application Express .	July 10, 2018
Amazon RDS for Oracle supports publishing logs to Amazon CloudWatch Logs (p. 2157)	Amazon RDS for Oracle now supports publishing alert, audit, trace, and listener log data to a log group in CloudWatch Logs. For more information, see Publishing Oracle logs to Amazon CloudWatch Logs .	July 9, 2018

MariaDB 10.2.15, 10.1.34, and 10.0.35 (p. 2157)	You can now create Amazon RDS DB instances running MariaDB versions 10.2.15, 10.1.34, and 10.0.35. For more information, see MariaDB on Amazon RDS versions .	July 5, 2018
Aurora PostgreSQL 1.2 is available and compatible with PostgreSQL 9.6.8 (p. 2157)	Aurora PostgreSQL 1.2 is now available and is compatible with PostgreSQL 9.6.8. For more information, see Version 1.2 .	June 27, 2018
Read replicas for Amazon RDS PostgreSQL support Multi-AZ deployments (p. 2157)	RDS read replicas in Amazon RDS PostgreSQL now support multiple Availability Zones. For more information, see Working with PostgreSQL read replicas .	June 25, 2018
Performance Insights available for Aurora PostgreSQL (p. 2157)	Performance Insights is generally available for Aurora PostgreSQL, with support for extended retention of performance data. For more information, see Using Amazon RDS performance insights .	June 21, 2018
Aurora PostgreSQL available in western US (northern California) region (p. 2157)	Aurora PostgreSQL is now available in the western United States (Northern California) region. For more information, see Availability for Amazon Aurora PostgreSQL .	June 11, 2018
Amazon RDS for Oracle now supports CPU configuration (p. 2157)	Amazon RDS for Oracle supports configuring the number of CPU cores and the number of threads for each core for the processor of a DB instance class. For more information, see Configuring the processor of the DB instance class .	June 5, 2018

Earlier updates

The following table describes the important changes in each release of the *Amazon RDS User Guide* before June 2018.

Change	Description	Date changed
Amazon RDS for PostgreSQL now supports PostgreSQL Version 11 Beta 1 in the	<p>PostgreSQL version 11 Beta 1 contains several improvements that are described in PostgreSQL 11 beta 1 released!</p> <p>For information on the Database Preview Environment, see Working with the database preview environment (p. 1802).</p>	May 31, 2018

Change	Description	Date changed
Database Preview Environment		
Amazon RDS for Oracle now supports TLS versions 1.0 and 1.2	Amazon RDS for Oracle supports Transport Layer Security (TLS) versions 1.0 and 1.2. For more information, see TLS versions for the Oracle SSL option (p. 1722) .	May 30, 2018
Aurora MySQL supports publishing logs to Amazon CloudWatch Logs	Aurora MySQL now supports publishing general, slow, audit, and error log data to a log group in CloudWatch Logs. For more information, see Publishing Aurora MySQL to CloudWatch Logs .	May 23, 2018
Database Preview Environment for Amazon RDS PostgreSQL	You can now launch a new instance of Amazon RDS PostgreSQL in a preview mode. For more information about the Database Preview Environment see, Working with the database preview environment (p. 1802) .	May 22, 2018
Amazon RDS for Oracle DB instances support new DB instance classes	Oracle DB instances now support the db.x1e and db.x1 DB instance classes. For more information, see DB instance classes (p. 10) and RDS for Oracle instance classes (p. 1477) .	May 22, 2018
Amazon RDS PostgreSQL now supports postgres_fdw on a read replica.	You can now use postgres_fdw to connect to a remote server from a read replica. For more information see, Using the postgres_fdw extension to access external data (p. 1988) .	May 17, 2018
Amazon RDS for Oracle now supports setting sqlnet.ora parameters	You can now set sqlnet.ora parameters with Amazon RDS for Oracle. For more information, see Modifying connection properties using sqlnet.ora parameters (p. 1494) .	May 10, 2018
Aurora PostgreSQL available in Asia Pacific (Seoul) region.	Aurora PostgreSQL is now available in the Asia Pacific (Seoul) region. For more information, see Availability for Amazon Aurora PostgreSQL .	May 9, 2018
Aurora MySQL supports backtracking	Aurora MySQL now supports "rewinding" a DB cluster to a specific time, without restoring data from a backup. For more information, see Backtracking an Aurora DB cluster .	May 9, 2018
Aurora MySQL supports encrypted migration and replication from external MySQL	Aurora MySQL now supports encrypted migration and replication from an external MySQL database. For more information, see Migrating data from an external MySQL database to an Amazon Aurora MySQL DB cluster and Replication between Aurora and MySQL or between Aurora and another Aurora DB cluster .	April 25, 2018
Aurora PostgreSQL-Compatible Edition support for the Copy-on-Write protocol.	You can now clone databases in an Aurora PostgreSQL database cluster. For more information see, Cloning databases in an Aurora DB cluster .	April 10, 2018

Change	Description	Date changed
MariaDB 10.2.12, 10.1.31, and 10.0.34	You can now create Amazon RDS DB instances running MariaDB versions 10.2.12, 10.1.31, and 10.0.34. For more information, see MariaDB on Amazon RDS versions (p. 982) .	March 21, 2018
Aurora PostgreSQL Support for new regions	Aurora PostgreSQL is now available in the EU (London) and Asia Pacific (Singapore) regions. For more information, see Availability for Amazon Aurora PostgreSQL .	March 13, 2018
MySQL 5.7.21, 5.6.39, and 5.5.59	You can now create Amazon RDS DB instances running MySQL versions 5.7.21, 5.6.39, and 5.5.59. For more information, see MySQL on Amazon RDS versions (p. 1315) .	March 9, 2018
Amazon RDS for Oracle now supports Oracle REST Data Services	Amazon RDS for Oracle supports Oracle REST Data Services as part of the APEX option. For more information, see Oracle Application Express (APEX) (p. 1664) .	March 9, 2018
Amazon Aurora MySQL-Compatible Edition available in new AWS Region	Aurora MySQL is now available in the Asia Pacific (Singapore) region. For the complete list of AWS Regions for Aurora MySQL, see Availability for Amazon Aurora MySQL .	March 6, 2018
Amazon RDS DB instances running Microsoft SQL Server support change data capture (CDC)	DB instances running Amazon RDS for Microsoft SQL Server now support change data capture (CDC). For more information, see Change data capture support for Microsoft SQL Server DB instances (p. 1070) .	February 6, 2018
Aurora MySQL supports a new major version	You can now create Aurora MySQL DB clusters running MySQL version 5.7. For more information, see Amazon Aurora MySQL database engine updates 2018-02-06 .	February 6, 2018
Publish MySQL and MariaDB logs to Amazon CloudWatch Logs	You can now publish MySQL and MariaDB log data to CloudWatch Logs. For more information, see Publishing MySQL logs to Amazon CloudWatch Logs (p. 703) and Publishing MariaDB logs to Amazon CloudWatch Logs (p. 689) .	January 17, 2018
Multi-AZ support for read replicas	You can now create a read replica as a Multi-AZ DB instance. Amazon RDS creates a standby of your replica in another Availability Zone for failover support for the replica. Creating your read replica as a Multi-AZ DB instance is independent of whether the source database is a Multi-AZ DB instance. For more information, see Working with read replicas (p. 370) .	January 11, 2018
Amazon RDS for MariaDB supports a new major version	You can now create Amazon RDS DB instances running MariaDB version 10.2. For more information, see MariaDB 10.2 support on Amazon RDS (p. 978) .	January 3, 2018

Change	Description	Date changed
Amazon Aurora PostgreSQL-Compatible Edition available in new AWS Region	Aurora PostgreSQL is now available in the EU (Paris) region. For the complete list of AWS Regions for Aurora PostgreSQL, see Availability for Amazon Aurora PostgreSQL .	December 22, 2017
Aurora PostgreSQL supports new instance types	Aurora PostgreSQL now supports new instance types. For the complete list of instance types, see Choosing the DB instance class .	December 20, 2017
Amazon Aurora MySQL-Compatible Edition available in new AWS Region	Aurora MySQL is now available in the EU (Paris) region. For the complete list of AWS Regions for Aurora MySQL, see Availability for Amazon Aurora MySQL .	December 18, 2017
Aurora MySQL supports hash joins	This feature can improve query performance when you need to join a large amount of data by using an equijoin. For more information, see Working with hash joins in Aurora MySQL .	December 11, 2017
Aurora MySQL supports native functions to invoke AWS Lambda functions	You can call the native functions <code>lambda_sync</code> and <code>lambda_async</code> when you use Aurora MySQL. For more information, see Invoking a Lambda function from an Amazon Aurora MySQL DB cluster .	December 11, 2017
Added Aurora PostgreSQL HIPAA eligibility	Aurora PostgreSQL now supports building HIPAA compliant applications. For more information, see Working with Amazon Aurora PostgreSQL .	December 6, 2017
Additional AWS Regions available for Amazon Aurora with PostgreSQL compatibility	Amazon Aurora with PostgreSQL compatibility is now available in four new AWS Regions. For more information, see Availability for Amazon Aurora PostgreSQL .	November 22, 2017
Modify storage for Amazon RDS DB instances running Microsoft SQL Server	You can now modify the storage of your Amazon RDS DB instances running SQL Server. For more information, see Modifying an Amazon RDS DB instance (p. 327) .	November 21, 2017
Amazon RDS supports 16 TiB storage for Linux-based engines	You can now create MySQL, MariaDB, PostgreSQL, and Oracle RDS DB instances with up to 16 TiB of storage. For more information, see Amazon RDS DB instance storage (p. 64) .	November 21, 2017
Amazon RDS supports fast scale up of storage	You can now add storage to MySQL, MariaDB, PostgreSQL, and Oracle RDS DB instances in a few minutes. For more information, see Amazon RDS DB instance storage (p. 64) .	November 21, 2017
Amazon RDS supports MariaDB versions 10.1.26 and 10.0.32	You can now create Amazon RDS DB instances running MariaDB versions 10.1.26 and 10.0.32. For more information, see MariaDB on Amazon RDS versions (p. 982) .	November 20, 2017

Change	Description	Date changed
Amazon RDS for Microsoft SQL Server now supports new DB instance classes	You can now create Amazon RDS DB instances running SQL Server that use the db.r4 and db.m4.16xlarge DB instance classes. For more information, see DB instance class support for Microsoft SQL Server (p. 1062) .	November 20, 2017
Amazon RDS for MySQL and MariaDB now supports new DB instance classes	You can now create Amazon RDS DB instances running MySQL and MariaDB that use the db.r4, db.m4.16xlarge, db.t2.xlarge, and db.t2.2xlarge DB instance classes. For more information, see DB instance classes (p. 10) .	November 20, 2017
SQL Server 2017	You can now create Amazon RDS DB instances running Microsoft SQL Server 2017. You can also create DB instances running SQL Server 2016 SP1 CU5. For more information, see Amazon RDS for Microsoft SQL Server (p. 1058) .	November 17, 2017
Restore MySQL backups from Amazon S3	You can now create a backup of your on-premises database, store it on Amazon S3, and then restore the backup file onto a new Amazon RDS DB instance running MySQL. For more information, see Restoring a backup into a MySQL DB instance (p. 1361) .	November 17, 2017
Auto Scaling with Aurora Replicas	Amazon Aurora MySQL now supports Aurora Auto Scaling. Aurora Auto Scaling dynamically adjusts the number of Aurora Replicas based on increases or decreases in connectivity or workload. For more information, see Using Amazon Aurora Auto Scaling with Aurora replicas .	November 17, 2017
Oracle default edition support	Amazon RDS for Oracle DB instances now supports setting the default edition for the DB instance. For more information, see Setting the default edition for a DB instance (p. 1553) .	November 3, 2017
Oracle DB instance file validation	Amazon RDS for Oracle DB instances now supports validating DB instance files with the Oracle Recovery Manager (RMAN) logical validation utility. For more information, see Validating DB instance files (p. 1571) .	November 3, 2017
Management Agent for OEM 13c	Amazon RDS for Oracle DB instances now support the Management Agent for Oracle Enterprise Manager (OEM) Cloud Control 13c. For more information, see Oracle Management Agent for Enterprise Manager Cloud Control (p. 1693) .	November 1, 2017
Storage reconfiguration for Microsoft SQL Server snapshots	You can now reconfigure the storage when you restore a snapshot to an Amazon RDS DB instance running Microsoft SQL Server. For more information, see Restoring from a DB snapshot (p. 452) .	October 26, 2017
Asynchronous key prefetch for Aurora MySQL-Compatible Edition	Asynchronous key prefetch (AKP) improves the performance of noncached index joins, by prefetching keys in memory ahead of when they are needed. For more information, see Working with asynchronous key prefetch in Amazon Aurora .	October 26, 2017

Change	Description	Date changed
MySQL 5.7.19, 5.6.37, and 5.5.57	You can now create Amazon RDS DB instances running MySQL versions 5.7.19, 5.6.37, and 5.5.57. For more information, see MySQL on Amazon RDS versions (p. 1315) .	October 25, 2017
General availability of Amazon Aurora with PostgreSQL compatibility	Amazon Aurora with PostgreSQL compatibility makes it simple and cost-effective to set up, operate, and scale your new and existing PostgreSQL deployments, thus freeing you to focus on your business and applications. For more information, see Working with Amazon Aurora PostgreSQL .	October 24, 2017
Amazon RDS for Oracle DB instances support new DB instance classes	Amazon RDS for Oracle DB instances now support memory optimized next generation (db.r4) instance classes. Amazon RDS for Oracle DB instances also now support the following new current generation instance classes: db.m4.16xlarge, db.t2.xlarge, and db.t2.2xlarge. For more information, see DB instance classes (p. 10) and RDS for Oracle instance classes (p. 1477) .	October 23, 2017
New feature	Your new and existing Reserved Instances can now cover multiple sizes in the same DB instance class. Size-flexible reserved instances are available for DB instances with the same AWS Region, database engine, and instance family, and across AZ configuration. Size-flexible reserved instances are available for the following database engines: Amazon Aurora, MariaDB, MySQL, Oracle (Bring Your Own License), PostgreSQL. For more information, see Size-flexible reserved DB instances (p. 141) .	October 11, 2017
New feature	You can now use the Oracle SQLT option to tune a SQL statement for optimal performance. For more information, see Oracle SQLT (p. 1733) .	September 22, 2017
New feature	If you have existing manual DB snapshots of your Amazon RDS for Oracle DB instances, you can now upgrade them to a later version of the Oracle database engine. For more information, see Upgrading an Oracle DB snapshot (p. 1764) .	September 20, 2017
New feature	You can now use Oracle Spatial to store, retrieve, update, and query spatial data in your Amazon RDS DB instances running Oracle. For more information, see Oracle Spatial (p. 1730) .	September 15, 2017
New feature	You can now use Oracle Locator to support internet and wireless service-based applications and partner-based GIS solutions with your Amazon RDS DB instances running Oracle. For more information, see Oracle Locator (p. 1706) .	September 15, 2017
New feature	You can now use Oracle Multimedia to store, manage, and retrieve images, audio, video, and other heterogeneous media data in your Amazon RDS DB instances running Oracle. For more information, see Oracle Multimedia (p. 1709) .	September 15, 2017

Change	Description	Date changed
New feature	You can now export audit logs from your Amazon Aurora MySQL DB clusters to Amazon CloudWatch Logs. For more information, see Publishing Aurora MySQL logs to Amazon CloudWatch Logs .	September 14, 2017
New feature	Amazon RDS now supports multiple versions of Oracle Application Express (APEX) for your DB instances running Oracle. For more information, see Oracle Application Express (APEX) (p. 1664) .	September 13, 2017
New feature	You can now use Amazon Aurora to migrate an unencrypted or encrypted DB snapshot or MySQL DB instance to an encrypted Aurora MySQL DB cluster. For more information, see Migrating an RDS for MySQL snapshot to Aurora and Migrating data from a MySQL DB instance to an Amazon Aurora MySQL DB cluster by using an Aurora read replica .	September 5, 2017
New feature	You can use Amazon RDS for Microsoft SQL Server databases to build HIPAA-compliant applications. For more information, see Compliance program support for Microsoft SQL Server DB instances (p. 1065) .	August 31, 2017
New feature	You can now use Amazon RDS for MariaDB databases to build HIPAA-compliant applications. For more information, see Amazon RDS for MariaDB (p. 974) .	August 31, 2017
New feature	You can now create Amazon RDS DB instances running Microsoft SQL Server with allocated storage up to 16 TiB, and Provisioned IOPS to storage ranges of 1:1–50:1. For more information, see Amazon RDS DB instance storage (p. 64) .	August 22, 2017
New feature	You can now use Multi-AZ deployments for DB instances running Microsoft SQL Server in the EU (Frankfurt) region. For more information, see Multi-AZ deployments for Amazon RDS for Microsoft SQL Server (p. 1129) .	August 3, 2017
New feature	You can now create Amazon RDS DB instances running MariaDB versions 10.1.23 and 10.0.31. For more information, see MariaDB on Amazon RDS versions (p. 982) .	July 17, 2017
New feature	Amazon RDS now supports Microsoft SQL Server Enterprise Edition with the License Included model in all AWS Regions. For more information, see Licensing Microsoft SQL Server on Amazon RDS (p. 1083) .	July 13, 2017

Change	Description	Date changed
New feature	Amazon RDS for Oracle now supports Linux kernel huge pages for increased database scalability. The use of huge pages results in smaller page tables and less CPU time spent on memory management, increasing the performance of large database instances. You can use huge pages with your Amazon RDS DB instances running all editions of Oracle versions 12.1.0.2 and 11.2.0.4. For more information, see Turning on HugePages for an RDS for Oracle instance (p. 1610) .	July 7, 2017
New feature	Updated to support encryption at rest (EAR) for db.t2.small and db.t2.medium DB instance classes for all non-Aurora DB engines. For more information, see Availability of Amazon RDS encryption (p. 2003) .	June 27, 2017
New feature	Updated to support Amazon Aurora in the Europe (Frankfurt) region. For more information, see Availability for Amazon Aurora MySQL .	June 16, 2017
New feature	You can now specify an option group when you copy a DB snapshot across AWS regions. For more information, see Option group considerations (p. 463) .	June 12, 2017
New feature	You can now copy DB snapshots created from specialized DB instances across AWS regions. You can copy snapshots from DB instances that use Oracle TDE, Microsoft SQL Server TDE, and Microsoft SQL Server Multi-AZ with Mirroring. For more information, see Copying a DB snapshot (p. 464) .	June 12, 2017
New feature	Amazon Aurora now allows you to quickly and cost-effectively copy all of your databases in an Amazon Aurora DB cluster. For more information, see Cloning databases in an Aurora DB cluster .	June 12, 2017
New feature	Amazon RDS now supports Microsoft SQL Server 2016 SP1 CU2. For more information, see Amazon RDS for Microsoft SQL Server (p. 1058) .	June 7, 2017
Preview	Public preview of Amazon Aurora with PostgreSQL Compatibility. For more information, see Working with Amazon Aurora PostgreSQL .	April 19, 2017
New feature	Amazon Aurora now allows you to run an ALTER TABLE <i>tbl_name</i> ADD COLUMN <i>col_name column_definition</i> operation nearly instantaneously. The operation completes without requiring the table to be copied and without materially impacting other DML statements. For more information, see Altering tables in Amazon Aurora using fast DDL .	April 5, 2017
New feature	We have added a new monitoring command, SHOW VOLUME STATUS, to display the number of nodes and disks in a volume. For more information, see Displaying volume status for an Aurora DB cluster .	April 5, 2017

Change	Description	Date changed
New feature	You can now use your own custom logic in your custom password verification functions for Oracle on Amazon RDS. For more information, see Creating custom functions to verify passwords (p. 1536) .	March 21, 2017
New feature	You can now access your online and archived redo log files on your Oracle DB instances on Amazon RDS. For more information, see Accessing online and archived redo logs (p. 1566) .	March 21, 2017
New feature	You can now copy both encrypted and unencrypted DB cluster snapshots between accounts in the same region. For more information, see Copying a DB cluster snapshot across accounts .	March 7, 2017
New feature	You can now share encrypted DB cluster snapshots between accounts in the same region. For more information, see Sharing a DB cluster snapshot .	March 7, 2017
New feature	You can now replicate encrypted Amazon Aurora MySQL DB clusters to create cross-region Aurora Replicas. For more information, see Replicating Aurora MySQL DB clusters across AWS Regions .	March 7, 2017
New feature	You can now require that all connections to your DB instance running Microsoft SQL Server use Secure Sockets Layer (SSL). For more information, see Using SSL with a Microsoft SQL Server DB instance (p. 1135) .	February 27, 2017
New feature	You can now set your local time zone to one of 15 additional time zones. For more information, see Supported time zones (p. 1075) .	February 27, 2017
New feature	You can now use the Amazon RDS procedure <code>msdb.dbo.rds_shrink_tempdbfile</code> to shrink the tempdb database on your DB instances running Microsoft SQL Server. For more information, see Shrinking the tempdb database (p. 1292) .	February 17, 2017
New feature	You can now compress your backup file when you export your Enterprise and Standard Edition Microsoft SQL Server database from an Amazon RDS DB instance to Amazon S3. For more information, see Compressing backup files (p. 1115) .	February 17, 2017
New feature	Amazon RDS now supports custom DNS servers to resolve DNS names used in outbound network access on your DB instances running Oracle. For more information, see Setting up a custom DNS server (p. 1539) .	January 26, 2017
New feature	Amazon RDS now supports creating an encrypted read replica in another region. For more information, see Creating a read replica in a different AWS Region (p. 383) and CreateDBInstanceReadReplica .	January 23, 2017

Change	Description	Date changed
New feature	Amazon RDS now supports upgrading a MySQL DB snapshot from MySQL 5.1 to MySQL 5.5. For more information, see Upgrading a MySQL DB snapshot (p. 1353) and ModifyDBSnapshot .	January 20, 2017
New feature	Amazon RDS now supports copying an encrypted DB snapshot to another region for the MariaDB, MySQL, Oracle, PostgreSQL, and Microsoft SQL Server database engines. For more information, see Copying a DB snapshot (p. 464) and CopyDBSnapshot .	December 20, 2016
New feature	Amazon Aurora MySQL now supports spatial indexing. Spatial indexing improves query performance on large datasets for queries that use spatial data. For more information, see Amazon Aurora MySQL and spatial data .	December 14, 2016
New feature	Amazon RDS now supports outbound network access on your DB instances running Oracle. You can use <code>utl_http</code> , <code>utl_tcp</code> , and <code>utl_smtp</code> to connect from your DB instance to the network. For more information, see Configuring UTL_HTTP access using certificates and an Oracle wallet (p. 1513) .	December 5, 2016
New feature	Amazon RDS has retired support for MySQL version 5.1. However, you can restore existing MySQL 5.1 snapshots to a MySQL 5.5 instance. For more information, see Supported storage engines for RDS for MySQL (p. 1312) .	November 15, 2016
New feature	Amazon RDS now supports Microsoft SQL Server 2016 RTM CU2. For more information, see Amazon RDS for Microsoft SQL Server (p. 1058) .	November 4, 2016
New feature	Amazon RDS now supports major version upgrades for DB instances running Oracle. You can now upgrade your Oracle DB instances from 11g to 12c. For more information, see Upgrading the RDS for Oracle DB engine (p. 1757) .	November 2, 2016
New feature	You can now create DB instances running Microsoft SQL Server 2014 Enterprise Edition. Amazon RDS now supports SQL Server 2014 SP2 for all editions and all regions. For more information, see Amazon RDS for Microsoft SQL Server (p. 1058) .	October 25, 2016
New feature	Amazon Aurora MySQL now integrates with other AWS services: You can load text or XML data into a table from an Amazon S3 bucket, or invoke an AWS Lambda function from database code. For more information, see Integrating Aurora MySQL with other AWS services .	October 18, 2016

Change	Description	Date changed
New feature	You can now access the tempdb database on your Amazon RDS DB instances running Microsoft SQL Server. You can access the tempdb database by using Transact-SQL through Microsoft SQL Server Management Studio (SSMS), or any other standard SQL client application. For more information, see Accessing the tempdb database on Microsoft SQL Server DB instances on Amazon RDS (p. 1292) .	September 29, 2016
New feature	You can now use the UTL_MAIL package with your Amazon RDS DB instances running Oracle. For more information, see Oracle UTL_MAIL (p. 1753) .	September 20, 2016
New features	You can now set the time zone of your new Microsoft SQL Server DB instances to a local time zone, to match the time zone of your applications. For more information, see Local time zone for Microsoft SQL Server DB instances (p. 1074) .	September 19, 2016
New feature	You can now use the Oracle Label Security option to control access to individual table rows in your Amazon RDS DB instances running Oracle Database 12c. With Oracle Label Security, you can enforce regulatory compliance with a policy-based administration model, and ensure that an access to sensitive data is restricted to only users with the appropriate clearance level. For more information, see Oracle Label Security (p. 1703) .	September 8, 2016
New feature	You can now connect to an Amazon Aurora DB cluster using the reader endpoint, which load-balances connections across the Aurora Replicas that are available in the DB cluster. As clients request new connections to the reader endpoint, Aurora distributes the connection requests among the Aurora Replicas in the DB cluster. This functionality can help balance your read workload across multiple Aurora Replicas in your DB cluster. For more information, see Amazon Aurora endpoints .	September 8, 2016
New feature	You can now support the Oracle Enterprise Manager Cloud Control on your Amazon RDS DB instances running Oracle. You can enable the Management Agent on your DB instances, and share data with your Oracle Management Service (OMS). For more information, see Oracle Management Agent for Enterprise Manager Cloud Control (p. 1693) .	September 1, 2016
New feature	This release adds support to get an ARN for a resource. For more information, see Getting an existing ARN (p. 406) .	August 23, 2016
New feature	You can now assign up to 50 tags for each Amazon RDS resource, for managing your resources and tracking costs. For more information, see Tagging Amazon RDS resources (p. 392) .	August 19, 2016

Change	Description	Date changed
New feature	<p>Amazon RDS now supports the License Included model for Oracle Standard Edition Two. For more information, see Creating an Amazon RDS DB instance (p. 230).</p> <p>You can now change the license model of your Amazon RDS DB instances running Microsoft SQL Server and Oracle. For more information, see Licensing Microsoft SQL Server on Amazon RDS (p. 1083) and RDS for Oracle licensing options (p. 1474).</p>	August 5, 2016
New feature	<p>Amazon RDS now supports native backup and restore for Microsoft SQL Server databases using full backup files (.bak files). You can now easily migrate SQL Server databases to Amazon RDS, and import and export databases in a single, easily-portable file, using Amazon S3 for storage, and AWS KMS for encryption. For more information, see Importing and exporting SQL Server databases using native backup and restore (p. 1099).</p>	July 27, 2016
New feature	<p>You can now copy the source files from a MySQL database to an Amazon Simple Storage Service (Amazon S3) bucket, and then restore an Amazon Aurora DB cluster from those files. This option can be considerably faster than migrating data using mysqldump. For more information, see Migrating data from an external MySQL database to an Aurora MySQL DB cluster.</p>	July 20, 2016
New feature	<p>You can now restore an unencrypted Amazon Aurora DB cluster snapshot to create an encrypted Amazon Aurora DB cluster by including an AWS Key Management Service (AWS KMS) encryption key during the restore operation. For more information, see Encrypting Amazon RDS resources.</p>	June 30, 2016
New feature	<p>You can use the Oracle Repository Creation Utility (RCU) to create a repository on Amazon RDS for Oracle. For more information, see Using the Oracle Repository Creation Utility on RDS for Oracle (p. 1786).</p>	June 17, 2016
New feature	<p>Adds support for PostgreSQL cross-region read replicas. For more information, see Creating a read replica in a different AWS Region (p. 383).</p>	June 16, 2016
New feature	<p>You can now use the AWS Management Console to easily add Multi-AZ with Mirroring to a Microsoft SQL Server DB instance. For more information, see Adding Multi-AZ to a Microsoft SQL Server DB instance (p. 1130).</p>	June 9, 2016
New feature	<p>You can now use Multi-AZ Deployments Using SQL Server Mirroring in the following additional regions: Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo). For more information, see Multi-AZ deployments for Amazon RDS for Microsoft SQL Server (p. 1129).</p>	June 9, 2016
New feature	<p>Updated to support MariaDB version 10.1. For more information, see Amazon RDS for MariaDB (p. 974).</p>	June 1, 2016

Change	Description	Date changed
New feature	Updated to support Amazon Aurora cross-region DB clusters that are read replicas. For more information, see Replicating Aurora MySQL DB clusters across AWS Regions .	June 1, 2016
New feature	Enhanced Monitoring is now available for Oracle DB instances. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) and Modifying an Amazon RDS DB instance (p. 327) .	May 27, 2016
New feature	Updated to support manual snapshot sharing for Amazon Aurora DB cluster snapshots. For more information, see Sharing a DB cluster snapshot .	May 18, 2016
New feature	You can now use the MariaDB Audit Plugin to log database activity on MariaDB and MySQL database instances. For more information, see Options for MariaDB database engine (p. 1040) and Options for MySQL DB instances (p. 1416) .	April 27, 2016
New feature	In-place, major version upgrades are now available for upgrading from MySQL version 5.6 to version 5.7. For more information, see Upgrading the MySQL DB engine (p. 1343) .	April 26, 2016
New feature	Enhanced Monitoring is now available for Microsoft SQL Server DB instances. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) .	April 22, 2016
New feature	Updated to provide an Amazon Aurora Clusters view in the Amazon RDS console. For more information, see Viewing an Aurora DB cluster .	April 1, 2016
New feature	Updated to support SQL Server Multi-AZ with mirroring in the Asia Pacific (Seoul) region. For more information, see Multi-AZ deployments for Amazon RDS for Microsoft SQL Server (p. 1129) .	March 31, 2016
New feature	Updated to support Amazon Aurora Multi-AZ with mirroring in the Asia Pacific (Seoul) region. For more information, see Availability for Amazon Aurora MySQL .	March 31, 2016
New feature	PostgreSQL DB instances have the ability to require connections to use SSL. For more information, see Using SSL with a PostgreSQL DB instance (p. 1816) .	March 25, 2016
New feature	Enhanced Monitoring is now available for PostgreSQL DB instances. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) .	March 25, 2016
New feature	Microsoft SQL Server DB instances can now use Windows Authentication for user authentication. For more information, see Using Windows Authentication with an Amazon RDS for SQL Server DB instance (p. 1143) .	March 23, 2016

Change	Description	Date changed
New feature	Enhanced Monitoring is now available in the Asia Pacific (Seoul) region. For more information, see Monitoring OS metrics with Enhanced Monitoring (p. 600) .	March 16, 2016
New feature	You can now customize the order in which Aurora Replicas are promoted to primary instance during a failover. For more information, see Fault tolerance for an Aurora DB cluster .	March 14, 2016
New feature	Updated to support encryption when migrating to an Aurora DB cluster. For more information, see Migrating data to an Aurora DB cluster .	March 2, 2016
New feature	Updated to support local time zone for Aurora DB clusters. For more information, see Local time zone for Aurora DB clusters .	March 1, 2016
New feature	Updated to add support for MySQL version 5.7 for current generation Amazon RDS DB instance classes.	February 22, 2016
New feature	Updated to support <i>db.r3</i> and <i>db.t2</i> DB instance classes in the AWS GovCloud (US-West) region.	February 11, 2016
New feature	Updated to support encrypting copies of DB snapshots and sharing encrypted DB snapshots. For more information, see Copying a DB snapshot (p. 458) and Sharing a DB snapshot (p. 472) .	February 11, 2016
New feature	Updated to support Amazon Aurora in the Asia Pacific (Sydney) region. For more information, see Availability for Amazon Aurora MySQL .	February 11, 2016
New feature	Updated to support SSL for Oracle DB Instances. For more information, see Using SSL with an RDS for Oracle DB instance (p. 1498) .	February 9, 2016
New feature	Updated to support local time zone for MySQL and MariaDB DB instances. For more information, see Local time zone for MySQL DB instances (p. 1433) and Local time zone for MariaDB DB instances (p. 1054) .	December 21, 2015
New feature	Updated to support Enhanced Monitoring of OS metrics for MySQL and MariaDB instances and Aurora DB clusters. For more information, see Viewing metrics in the Amazon RDS console (p. 525) .	December 18, 2015
New feature	Updated to support <i>db.t2</i> , <i>db.r3</i> , and <i>db.m4</i> DB instance classes for MySQL version 5.5. For more information, see DB instance classes (p. 10) .	December 4, 2015
New feature	Updated to support modifying the database port for an existing DB instance.	December 3, 2015
New feature	Updated to support major version upgrades of the database engine for PostgreSQL instances. For more information, see Upgrading the PostgreSQL DB engine for Amazon RDS (p. 1839) .	November 19, 2015

Change	Description	Date changed
New feature	Updated to support modifying the public accessibility of an existing DB instance. Updated to support db.m4 standard DB instance classes.	November 11, 2015
New feature	Updated to support manual DB snapshot sharing. For more information, see Sharing a DB snapshot (p. 472) .	October 28, 2015
New feature	Updated to support Microsoft SQL Server 2014 for the Web, Express, and Standard editions.	October 26, 2015
New feature	Updated to support the MySQL-based MariaDB database engine. For more information, see Amazon RDS for MariaDB (p. 974) .	October 7, 2015
New feature	Updated to support Amazon Aurora in the Asia Pacific (Tokyo) region. For more information, see Availability for Amazon Aurora MySQL .	October 7, 2015
New feature	Updated to support db.t2 burst-capable DB instance classes for all DB engines and the addition of the db.t2.large DB instance class. For more information, see DB instance classes (p. 10) .	September 25, 2015
New feature	Updated to support Oracle DB instances on R3 and T2 DB instance classes. For more information, see DB instance classes (p. 10) .	August 5, 2015
New feature	Microsoft SQL Server Enterprise Edition is now available with the License Included service model. For more information, see Licensing Microsoft SQL Server on Amazon RDS (p. 1083) .	July 29, 2015
New feature	Amazon Aurora has officially released. The Amazon Aurora DB engine supports multiple DB instances in a DB cluster. For detailed information, see What is Amazon Aurora? .	July 27, 2015
New feature	Updated to support copying tags to DB snapshots.	July 20, 2015
New feature	Updated to support increases in storage size for all DB engines and an increase in Provisioned IOPS for SQL Server.	June 18, 2015
New feature	Updated options for reserved DB instances.	June 15, 2015
New feature	Updated to support using Amazon CloudHSM with Oracle DB instances using TDE.	January 8, 2015
New feature	Updated to support encrypting data at rest and new API version 2014-10-31.	January 6, 2015
New feature	Updated to include the new Amazon DB engine: Aurora. The Amazon Aurora DB engine supports multiple DB instances in a DB cluster. Amazon Aurora is currently in preview release and is subject to change. For detailed information, see What is Amazon Aurora? .	November 12, 2014
New feature	Updated to support PostgreSQL read replicas.	November 10, 2014

Change	Description	Date changed
New API and features	Updated to support the GP2 storage type and new API version 2014-09-01. Updated to support the ability to copy an existing option or parameter group to create a new option or parameter group.	October 7, 2014
New feature	Updated to support InnoDB Cache Warming for DB instances running MySQL version 5.6.19 and later.	September 3, 2014
New feature	Updated to support SSL certificate verification when connecting to MySQL version 5.6, SQL Server, and PostgreSQL database engines.	August 5, 2014
New feature	Updated to support the db.t2 burstable DB instance classes.	August 4, 2014
New feature	Updated to support the db.r3 memory optimized DB instance classes for use with the MySQL (version 5.6), SQL Server, and PostgreSQL database engines.	May 28, 2014
New feature	Updated to support SQL Server Multi-AZ deployments using SQL Server Mirroring.	May 19, 2014
New feature	Updated to support upgrades from MySQL version 5.5 to version 5.6.	April 23, 2014
New feature	Updated to support Oracle GoldenGate.	April 3, 2014
New feature	Updated to support the M3 DB instance classes.	February 20, 2014
New feature	Updated to support the Oracle Timezone option.	January 13, 2014
New feature	Updated to support replication between MySQL DB instances in different regions.	November 26, 2013
New feature	Updated to support the PostgreSQL DB engine.	November 14, 2013
New feature	Updated to support SQL Server transparent data encryption (TDE).	November 7, 2013
New API and new feature	Updated to support cross region DB snapshot copies; new API version, 2013-09-09.	October 31, 2013
New features	Updated to support Oracle Statspack.	September 26, 2013
New features	Updated to support using replication to import or export data between instances of MySQL running in Amazon RDS and instances of MySQL running on-premises or on Amazon EC2.	September 5, 2013
New features	Updated to support the db.cr1.8xlarge DB instance class for MySQL 5.6.	September 4, 2013
New feature	Updated to support replication of read replicas.	August 28, 2013
New feature	Updated to support parallel read replica creation.	July 22, 2013
New feature	Updated to support fine-grained permissions and tagging for all Amazon RDS resources.	July 8, 2013

Change	Description	Date changed
New feature	Updated to support MySQL 5.6 for new instances, including support for the MySQL 5.6 memcached interface and binary log access.	July 1, 2013
New feature	Updated to support major version upgrades from MySQL 5.1 to MySQL 5.5.	June 20, 2013
New feature	Updated DB parameter groups to allow expressions for parameter values.	June 20, 2013
New API and new feature	Updated to support read replica status; new API version, 2013-05-15.	May 23, 2013
New features	Updated to support Oracle Advanced Security features for native network encryption and Oracle Transparent Data Encryption.	April 18, 2013
New features	Updated to support major version upgrades for SQL Server and additional functionality for Provisioned IOPS.	March 13, 2013
New feature	Updated to support VPC By Default for RDS.	March 11, 2013
New API and feature	Updated to support log access; new API version 2013-02-12	March 4, 2013
New feature	Updated to support RDS event notification subscriptions.	February 4, 2013
New API and feature	Updated to support DB instance renaming and the migration of DB security group members in a VPC to a VPC security group.	January 14, 2013
New feature	Updated for AWS GovCloud (US-West) support.	December 17, 2012
New feature	Updated to support m1.medium and m1.xlarge DB Instance classes.	November 6, 2012
New feature	Updated to support read replica promotion.	October 11, 2012
New feature	Updated to support SSL in Microsoft SQL Server DB Instances.	October 10, 2012
New feature	Updated to support Oracle micro DB Instances.	September 27, 2012
New feature	Updated to support SQL Server 2012.	September 26, 2012
New API and feature	Updated to support provisioned IOPS. API version 2012-09-17.	September 25, 2012
New features	Updated for SQL Server support for DB Instances in VPC and Oracle support for Data Pump.	September 13, 2012
New feature	Updated for support for SQL Server Agent.	August 22, 2012
New feature	Updated for support for tagging of DB Instances.	August 21, 2012
New features	Updated for support for Oracle APEX and XML DB, Oracle time zones, and Oracle DB Instances in a VPC.	August 16, 2012

Change	Description	Date changed
New features	Updated for support for SQL Server Database Engine Tuning Advisor and Oracle DB Instances in VPC.	July 18, 2012
New feature	Updated for support for option groups and first option, Oracle Enterprise Manager Database Control.	May 29, 2012
New feature	Updated for support for read replicas in Amazon Virtual Private Cloud.	May 17, 2012
New feature	Updated for Microsoft SQL Server support.	May 8, 2012
New features	Updated for support for forced failover, Multi-AZ deployment of Oracle DB Instances, and nondefault character sets for Oracle DB Instances.	May 2, 2012
New feature	Updated for Amazon Virtual Private Cloud (VPC) Support.	February 13, 2012
Updated content	Updated for new Reserved Instance types.	December 19, 2011
New feature	Updated for Oracle engine support.	May 23, 2011
Updated content	Console updates.	May 13, 2011
Updated content	Edited content for shortened backup and maintenance windows.	February 28, 2011
New feature	Added support for MySQL 5.5.	January 31, 2011
New feature	Added support for read replicas.	October 4, 2010
New feature	Added support for AWS Identity and Access Management (IAM).	September 2, 2010
New feature	Added DB Engine Version Management.	August 16, 2010
New feature	Added Reserved DB Instances.	August 16, 2010
New Feature	Amazon RDS now supports SSL connections to your DB Instances.	June 28, 2010
New Guide	This is the first release of the Amazon RDS User Guide.	June 7, 2010

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.